September 11, 2018</br></br> We have completed our review. Please refer to the attached letter for details.

If you have any questions, please contact the lead reviewer assigned to your submission, Erdit Gremi.

 *** This is a system-generated email notification ***

September 11, 2018

Apple Inc.
% Donna-Bea Tillman
Senior Consultant
Biologics Consulting Group
1555 King St, Suite 300
Alexandria, Virginia 22314

Re: DEN180042
Trade/Device Name: Irregular Rhythm Notification Feature
Regulation Number: 21 CFR 870.2790
Regulation Name: Photoplethysmograph analysis software for over-the-counter use
Regulatory Class: Class II
Product Code: QDB
Dated: August 8, 2018
Received: August 9, 2018

Dear Donna-Bea Tillman:

The Center for Devices and Radiological Health (CDRH) of the Food and Drug Administration (FDA) has completed its review of your De Novo request for classification of the Irregular Rhythm Notification Feature, an over-the-counter device under 21 CFR Part 801 Subpart C with the following indications for use:

> The Irregular Rhythm Notification Feature is a software-only mobile medical application that is intended to be used with the Apple Watch. The feature analyzes pulse rate data to identify episodes of irregular heart rhythms suggestive of atrial fibrillation (AFib) and provides a notification to the user. The feature is intended for over-the-counter (OTC) use. It is not intended to provide a notification on every episode of irregular rhythm suggestive of AFib and the absence of a notification is not intended to indicate no disease process is present; rather the feature is intended to opportunistically surface a notification of possible AFib when sufficient data are available for analysis. These data are only captured when the user is still. Along with the user's risk factors, the feature can be used to supplement the decision for AFib screening. The feature is not intended to replace traditional methods of diagnosis or treatment.
>
> The feature has not been tested for and is not intended for use in people under 22 years of age. It is also not intended for use in individuals previously diagnosed with AFib.

FDA concludes that this device should be classified into Class II. This order, therefore, classifies the Irregular Rhythm Notification Feature, and substantially equivalent devices of this generic type, into Class II under the generic name photoplethysmograph analysis software for over-the-counter use.

FDA identifies this generic type of device as:

Photoplethysmograph analysis software for over-the-counter use. A photoplethysmograph analysis software device for over-the-counter use analyzes photoplethysmograph data and provides information for identifying irregular heart rhythms. This device is not intended to provide a diagnosis.

Section 513(f)(2) of the Food, Drug and Cosmetic Act (the FD&C Act) was amended by section 607 of the Food and Drug Administration Safety and Innovation Act (FDASIA) on July 9, 2012. This law provides two options for De Novo classification. First, any person who receives a "not substantially equivalent" (NSE) determination in response to a 510(k) for a device that has not been previously classified under the Act may request FDA to make a risk-based classification of the device under section 513(a)(1) of the Act. On December 13, 2016, the 21st Century Cures Act removed a requirement that a De Novo request be submitted within 30 days of receiving an NSE determination. Alternatively, any person who determines that there is no legally marketed device upon which to base a determination of substantial equivalence may request FDA to make a risk-based classification of the device under section 513(a)(1) of the Act without first submitting a 510(k). FDA shall, within 120 days of receiving such a request, classify the device. This classification shall be the initial classification of the device. Within 30 days after the issuance of an order classifying the device, FDA must publish a notice in the Federal Register announcing the classification.

On August 9, 2018, FDA received your De Novo requesting classification of the Irregular Rhythm Notification Feature. The request was submitted under section 513(f)(2) of the FD&C Act. In order to classify the Irregular Rhythm Notification Feature into class I or II, it is necessary that the proposed class have sufficient regulatory controls to provide reasonable assurance of the safety and effectiveness of the device for its intended use. After review of the information submitted in the De Novo request, FDA has determined that, for the previously stated indications for use, the Irregular Rhythm Notification Feature can be classified in class II with the establishment of special controls for class II. FDA believes that class II (special) controls provide reasonable assurance of the safety and effectiveness of the device type. The identified risks and mitigation measures associated with the device type are summarized in the following table:

Table 1 – Identified Risks to Health and Mitigation Measures

Identified Risk	**Mitigation Measures**
Poor quality incoming PPG signal resulting in failure to detect irregular heart rhythms	Clinical performance testing Human factors testing Labeling
Misinterpretation and/or over-reliance on device output, leading to: • Failure to seek treatment despite acute symptoms (e.g., fluttering sensation in the chest, lightheadedness, and irregular pulse) • Discontinuing or modifying treatment for chronic heart condition	Human factors testing Labeling
False negative resulting in failure to detect irregular heart rhythms and delay of further evaluation or treatment	Clinical performance testing Software verification, validation, and hazard analysis

	Non-clinical performance testing Labeling
False positive resulting in additional unnecessary medical procedures	Clinical performance testing Software verification, validation, and hazard analysis Non-clinical performance testing Labeling

In combination with the general controls of the FD&C Act, the photoplethysmograph analysis software for over-the-counter use is subject to the following special controls:

1. Clinical performance testing must demonstrate the performance characteristics of the detection algorithm under anticipated conditions of use.

2. Software verification, validation, and hazard analysis must be performed. Documentation must include a characterization of the technical specifications of the software, including the detection algorithm and its inputs and outputs.

3. Non-clinical performance testing must demonstrate the ability of the device to detect adequate PPG signal quality.

4. Human factors and usability testing must demonstrate the following:
    a. The user can correctly use the device based solely on reading the device labeling; and
    b. The user can correctly interpret the device output and understand when to seek medical care.

5. Labeling must include:
    a. Hardware platform and operating system requirements;
    b. Situations in which the device may not operate at an expected performance level;
    c. A summary of the clinical performance testing conducted with the device;
    d. A description of what the device measures and outputs to the user; and
    e. Guidance on interpretation of any results.

Section 510(m) of the FD&C Act provides that FDA may exempt a class II device from the premarket notification requirements under section 510(k) of the FD&C Act, if FDA determines that premarket notification is not necessary to provide reasonable assurance of the safety and effectiveness of the device type. FDA has determined premarket notification is necessary to provide reasonable assurance of the safety and effectiveness of the device type and, therefore, the device is not exempt from the premarket notification requirements of the FD&C Act. Thus, persons who intend to market this device type must submit a premarket notification containing information on the photoplethysmograph analysis software for over-the-counter use they intend to market prior to marketing the device.

Although this letter refers to your product as a device, please be aware that some granted products may instead be combination products. If you have questions on whether your product is a combination product, contact CDRHProductJurisdiction@fda.hhs.gov.

Please be advised that FDA's decision to grant this De Novo request does not mean that FDA has made a determination that your device complies with other requirements of the FD&C Act or any Federal statutes and regulations administered by other Federal agencies. You must comply with all the FD&C Act's requirements, including, but not limited to: registration and listing (21 CFR Part 807); labeling (21 CFR Part 801); medical device reporting (reporting of medical device-related adverse events) (21 CFR 803) for devices or postmarketing safety reporting (21 CFR 4, Subpart B) for combination products (see https://www.fda.gov/CombinationProducts/GuidanceRegulatoryInformation/ucm597488.htm); good manufacturing practice requirements as set forth in the quality systems (QS) regulation (21 CFR Part 820) for devices or current good manufacturing practices (21 CFR 4, Subpart A) for combination products; and if applicable, the electronic product radiation control provisions (Sections 531-542 of the FD&C Act); 21 CFR 1000-1050.

A notice announcing this classification order will be published in the Federal Register. A copy of this order and supporting documentation are on file in the Dockets Management Branch (HFA-305), Food and Drug Administration, 5630 Fishers Lane, Room 1061, Rockville, MD 20852 and are available for inspection between 9 a.m. and 4 p.m., Monday through Friday.

As a result of this order, you may immediately market your device as described in the De Novo request, subject to the general control provisions of the FD&C Act and the special controls identified in this order.

For comprehensive regulatory information about medical devices and radiation-emitting products, please see Device Advice (https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/) and CDRH Learn (http://www.fda.gov/Training/CDRHLearn). Additionally, you may contact the Division of Industry and Consumer Education (DICE) to ask a question about a specific regulatory topic. See the DICE website (http://www.fda.gov/DICE) for more information or contact DICE by email (DICE@fda.hhs.gov) or phone (1-800-638-2041 or 301-796-7100).

If you have any questions concerning the contents of the letter, please contact Erdit Gremi at 240-402-3910.

Sincerely,

Angela C. Krueger -S

Angela C. Krueger
Deputy Director, Engineering and Science Review
Office of Device Evaluation
Center for Devices and Radiological Health

DEN180042/A001

Biologics CONSULTING
PHARMACEUTICALS, DEVICES & BIOLOGICS ADVISORS

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

August 10, 2018

Re: DEN180042 - de novo Amendment
Submitter: (b) (4)
Device Name: (b) (4) App

Dear Erdit Gremi:

I am submitting this amendment to DEN180042 for the (b) (4), in accordance with the Modular Submission plan previously agreed to with FDA. This amendment ecopy contains the following files:

001_DEN180042_A1 Cover Letter
002_(b) (4) Clinical Study Report
003_Appendix A Signature Page
004_Appendix B_IRB Information
005_Appendix C_AHS Sub-Study Protocol
006_Appendix D_AHS Sub-study Statistical Analysis Plan
STATISTICAL DATA – contains zip files of raw data, listings, tables and SAS files

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of (b) (4) or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must comply with all provisions of 21 C.F.R. § 20.61(e), including by providing (b) (4) with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions or concerns, do not hesitate to reach out to me or other members of the team. We really appreciate the opportunity to work with you to explore novel approaches for digital health product premarket reviews.

Biologics Consulting Group, Inc.
1555 King Street, Suite 300 • Alexandria, Virginia 22314
Phone: 703.739.5695 • Toll Free: 800.485.0106 • Fax: 703.548.7457
BiologicsConsulting.com

Biologics CONSULTING | PHARMACEUTICALS, DEVICES & BIOLOGICS ADVISORS

Sincerely,

(b) (6)

Donna Bea Tillman, Ph.D.
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

August 10, 2018

Re: DEN180042 - de novo Amendment
Submitter: (b) (4)
Device Name: (b) (4) App

Dear Erdit Gremi:

I am submitting this amendment to DEN180042 for the (b) (4) App, in accordance with the (b) (4) plan previously agreed to with FDA. This amendment ecopy contains the following files:

001_DEN180042_A1 Cover Letter
002_(b) (4) Clinical Study Report
003_Appendix A Signature Page
004_Appendix B_IRB Information
005_Appendix C_AHS Sub-Study Protocol
006_Appendix D_AHS Sub-study Statistical Analysis Plan
STATISTICAL DATA – contains zip files of raw data, listings, tables and SAS files

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of (b) (4) or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must comply with all provisions of 21 C.F.R. § 20.61(e), including by providing (b) (4) with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions or concerns, do not hesitate to reach out to me or other members of the team. We really appreciate the opportunity to work with you to explore novel approaches for digital health product premarket reviews.

Biologics Consulting Group, Inc.
1555 King Street, Suite 300 • Alexandria, Virginia 22314
Phone: 703.739.5695 • Toll [illegible]
BiologicsConsulting.com

Biologics CONSULTING | PHARMACEUTICALS, DEVICES & BIOLOGICS ADVISORS

Sincerely,

(b) (6)

Donna Bea Tillman, Ph.D.
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

APPLE HEART STUDY SUB-STUDY

Clinical Study Report

August 7, 2018

Apple Inc.

This study was conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, clinical research guidelines established by the U.S. Food and Drug Administration (21 CFR Parts 50, 54, 56, and 812), and ICH GCP Guidelines.

TABLE OF CONTENTS

TABLES

LISTINGS

APPENDICES

1. LIST OF ABBREVIATIONS AND DEFINITIONS OF TERMS

The following abbreviations and specialist terms are used in this study report.

Abbreviation or Specialist Term	Explanation
ADE	Adverse Device Effect
AF	Atrial Fibrillation/Atrial Flutter
AHS	Apple Heart Study
AT	Atrial Tachycardia
CFR	Code of Federal Regulations
CRO	Clinical Research Organization
EAS	ECG Analysis Set
ECG	Electrocardiogram
FAS	Full Analysis Set
FDA	Food and Drug Administration
GCP	Good Clinical Practice
H_0	Null Hypothesis
H_A	Alternative Hypothesis
HRV	Heart Rate Variability
ICF	Informed Consent Form
ICH	International Conference on Harmonization
IRB	Institutional Review Board
J-Beat	Junctional Beats
SA	Sinus Arrhythmia
SAP	Statistical Analysis Plan
SR	Sinus Rhythm
PAC	Premature Atrial Contractions
PPG	Photoplethysmogram
PPV	Positive Predictive Value
PVC	Premature Ventricular Contractions
QC	Quality Control
VF	Ventricular Fibrillation
VT	Ventricular Tachycardia

2. PROTOCOL SYNOPSIS

Overview

This Apple Heart Study Sub-Study (AHS Sub-Study) Protocol describes the analysis that will be conducted on a subset of data from the ongoing Apple Heart Study. This AHS Sub-Study is being conducted to determine if the tachogram classification algorithm and confirmation cycle algorithm (alert-level) have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF) in a subset of AHS participants.

Study Objective

The objective of this AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF).

Study Endpoints

1. Primary Endpoint: Identification of irregular rhythm consistent with AF as suggested by positive predictive value (PPV) of the spot tachogram (Spot Tachogram PPV)
2. Secondary Endpoint: Identification of irregular rhythm consistent with AF as suggested by PPV of the notification (Alert-Level PPV)
3. Primary Safety Endpoint: Serious adverse device effects (ADEs)

Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b) (4)

H_0: $PPV_{Tachogram(AF)}$ (b) (4)

vs.

H_A: $PPV_{Tachogram(AF)}$ (b) (4)

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

Subject Population

AHS began on November 30, 2017. The data to support this sub-study will come from AHS participants who were enrolled between November 30, 2017, to June 22, 2018, who have received the ECG patch (ePatch provided by BioTelemetry) and for whom ECG data has been adjudicated. The analysis defined in this sub-study protocol will not be initiated until all participant data (up to June 22, 2018) to be used in the analysis is available.

To ensure the confidentiality of the subject data, subject data will be identified by a participant ID number for which the Sponsor will not have the ability to link back to the subject's identity. The

use of the data in this sub-study is consistent with the disclosure of research aims and use of the data made to the subjects in the IRB-approved Apple Heart Study informed consent form.

The inclusion/exclusion criteria for the AHS is as follows:

Inclusion Criteria

Subjects must meet all the following inclusion criteria to be enrolled:

1. Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:
   I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.
   II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.
2. Age ≥ 22 years at time of eligibility screening, ascertained from self-reported date of birth.
3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.
4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.
5. Valid phone number associated with iPhone, ascertained from self-report.
6. Valid email address, ascertained from self-report.

Exclusion Criteria

Subjects who meet any of the following criteria may not be enrolled:

1. Self-reported diagnosis of Atrial Fibrillation at time of consent.
2. Self-reported diagnosis of Atrial Flutter at time of consent.
3. Currently on anticoagulation therapy, as self-reported at the time of consent.

Sample Size

The sample size in this sub-study is the number of spot tachograms. (b) (4) [redacted]

3. ETHICS

3.1. Institutional Review Board

Using the Department of Health and Human Services regulations found at 45 CFR 46.101(b)(4), the Institutional Review Board (IRB) determined that the Apple Heart Study (AHS) Sub-Study is exempt from IRB oversight. Documentation of IRB-exempt status was obtained. Details of the IRB are provided in Appendix B.

3.2. Ethical Conduct of the Study

The AHS Sub-Study was designed and monitored in accordance with Sponsor procedures, which comply with the ethical principles of Good Clinical Practice (GCP) as required by the major regulatory authorities, and in accordance with the Declaration of Helsinki.

3.3. Informed Consent

Informed consent was obtained from all AHS participants from whom data is being used to support data analysis for the AHS Sub-Study. Study participants were informed that their study data could be used in the context of a regulatory submission and for commercial purposes. No additional informed consent for this sub-study was required.

Informed Consent Process in the Apple Heart Study (AHS)

The AHS is an ongoing app-based research study being conducted through the AHS app. As in other mobile-mediated research studies, the informed consent process in the AHS was conducted remotely in a completely self-administered setting with no required contact with the research team prior to consent and enrollment.

The potential participant first downloaded the AHS app. The app automatically ensured compatibility with the iPhone iOS version and Watch version. If compatible, the participant was able to continue forward in the app. An overview of the study was also displayed in the app.

The participant then advanced to a screen for study enrollment, where he/she confirmed whether general participation requirements were met. The participant was asked questions based on study inclusion and exclusion criteria. The app automatically determined eligibility based on the responses provided. If the participant was determined to be eligible, he/she was presented with an in-app consent and authorization form to be read and signed if the participant agreed to participate.

A copy of the signed study consent and authorization document was available for review and download to the participant via the app. After consenting to participate, the participant was directed to complete a brief questionnaire to collect self-reported baseline demographics and medical history. The participant was considered ‘enrolled’ from this point and the study app’s analysis of Apple Watch Photoplethysmogram (PPG) sensor data began thereafter.

The approach to informed consent for the AHS was meant to ensure that participants were adequately informed about the research before agreeing to participate. Potential candidates as well

as enrolled participants were able to contact an AHS hotline (available 24/7 at 1-844-606-1609) any time and had the ability to ask questions, request clarifications, or report a problem at any time prior to or during the study. This hotline was opened from the study start date and will remain open until study closure.

4. INVESTIGATORS AND STUDY ADMINISTRATIVE STRUCTURE

4.1. Investigators

Investigative sites were not utilized during this sub-study. This clinical study report (CSR) includes data from subjects who were enrolled between November 30, 2017, and June 22, 2018, who received an ePatch and for whom ECG data was adjudicated in the AHS, an app-based research study conducted in the United States.

4.2. Study Administrative Structure

4.2.1. Sponsor Responsibilities

The AHS Sub-study is an analysis on a pre-specified subset of data collected in the AHS to support a regulatory submission before the AHS ends. AHS is an app-based research non-significant risk study and was sponsored by Apple Inc. The Sponsor developed the protocol and statistical analysis plan (SAP) to conduct this sub-study.

The Sponsor's responsible Clinical/Regulatory Study Representative attested to the accuracy of this report and his/her signature is provided in Appendix A.

The Sponsor recruited and managed the contract research organizations (CROs).

4.2.2. Contract Research Organization (CRO) Responsibilities

Three independent ECG adjudicators (BioTelemetry, Inc., Malvern, PA) provided review and adjudication of ECG strips with oversight by the Sponsor.

The adjudicators were required to have U.S. board-certification in Cardiology and/or Electrophysiology, with extensive and relevant experience in clinical, clinical research, and/or event adjudication expertise as assessed by review of their CVs.

5. INTRODUCTION

5.1. Background

Atrial fibrillation (AF) is the most common serious cardiac arrhythmia, and, when left untreated, is a leading cause of morbidity and mortality from stroke, heart failure and myocardial infarction[1,2]. Data from the Framingham Heart Study indicates that by age 40 years, lifetime risk for developing AF is 1 in 4. AF is also a growing public health problem with prevalence projected to triple between 2010 and 2050, with an estimated 12.1 million diagnosed cases in 2030 in the United States alone.

Early detection and treatment of patients with AF minimizes the risk of sequelae of thromboembolism including >60% reduced risk of stroke[2]. However, many affected with AF are unaware they have this arrhythmia due to a number of factors, including lack of symptoms, or they may experience only mild symptoms that they do not attribute to a disease[2]. As a result, asymptomatic patients are 3 times as likely to have sustained an ischemic stroke prior to diagnosis than those with symptoms[1]. These findings raise concerns and have prompted several variations of screening programs to detect patients with asymptomatic AF to prevent an embolic event[1,2]. While systematic and opportunistic screening programs have demonstrated increased rates of detection when compared to detection during routine clinical practice, such screening programs are not yet widely implemented[2]. Additionally, AF may be paroxysmal (PAF, or intermittent AF) and therefore missed by recording a single in-clinic electrocardiogram (ECG). This is especially true for those patients with intermittent symptoms. Holter devices are commonly used for ambulatory 24-hour ECG monitoring in at-risk patients but have limited sensitivity for the detection of new AF[7].

5.2. Device Description and Purpose of the Sub-Study

This sub-study used data collected from a subset of participants enrolled in the *Apple Heart Study: Assessment of Wristwatch-Based Photoplethysmography to Identify Cardiac Arrhythmias*, which is a large, prospective, single arm, experimental non-significant risk study, conducted with the assistance of eligible participants without a known history of atrial fibrillation or atrial flutter (at the time of consent). The subjects in this sub-study received an irregular rhythm notification within the AHS App and consequently received and wore an ambulatory ECG patch (ePatch) for interpretation of the ambulatory ECG findings by trained ECG technicians.

The AHS app is a mobile medical application used in the ongoing AHS. Because the AHS study is being conducted completely virtually, the app functions as a means to screen for inclusion/exclusion criteria, collect the electronic informed consent, collect user information and medical history, and is used by the subjects to connect to a Study Telehealth Provider if they receive an irregular rhythm notification or if they need to report a problem (described in section above). The app also contains the tachogram classification algorithm and alert-level confirmation cycle algorithm, both of which were validated in this sub-study.

The tachogram classification algorithm classified a tachogram as irregular or not AF, and the alert-level confirmation cycle algorithm determined if a notification was surfaced to the user. At baseline, the Apple Watch platform attempted to capture a tachogram every 2-4 hours to support

the commercially available heart rate variability (HRV) feature, and the AHS app retrieved and analyzed any such tachograms that were captured. If a tachogram was classified as irregular, the "confirmation cycle" began, during which the AHS app requested additional tachograms from the platform more frequently (as frequently as possible, subject to a minimum spacing of 15 minutes). If five out of six sequential tachograms (including the initial one) were classified as irregular within a 48-hour period, a notification of this finding was surfaced to the user. If two tachograms were classified as not AF before this threshold was reached, the AHS app returned to baseline (attempting to retrieve tachograms every 2-4 hours), no results were surfaced, and the confirmation cycle was reset (that is, any irregular tachograms within this sequence did not count in future confirmation cycles).

When the AHS app surfaced the first notification to the user, the workflow to call the Study Telehealth Provider and receive the ambulatory ECG monitor (ePatch) was initiated. After the first notification was surfaced, no additional notifications were surfaced to the user. However, notifications continued to be generated for the purposes of data analysis ("silent notifications"). The classified tachograms that contributed to a notification and the notification itself were stored and used for the alert-level positive predictive value (PPV) analysis.

The tachogram and notification data collected and processed through the algorithms within the AHS app are the subject of this sub-study and were compared to the gold-standard ECG (ePatch) to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV. The data analyzed in this sub-study was obtained from AHS participants who were enrolled between November 30, 2017, and June 22, 2018, who received an ePatch and for whom ECG data was adjudicated. The AHS Sub-study analysis was conducted prior to the completion of the AHS.

6. STUDY OBJECTIVE

The objective of this AHS Sub-Study was to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV as compared to the ePatch monitoring in identifying irregular rhythms consistent with AF.

7. STUDY ENDPOINTS

7.1. Primary Efficacy Endpoint

The primary efficacy endpoint of this sub-study is the identification of irregular rhythm consistent with AF as suggested by PPV of the spot tachogram where the ePatch readings (paired to the timestamp associated with the spot tachograms) were used for the determination of AF. Each subject may have contributed multiple observations (i.e., spot tachograms) for this endpoint.

7.2. Secondary Efficacy Endpoint

The secondary efficacy endpoint is the identification of irregular rhythm consistent with AF as suggested by PPV of the alert (based on multiple irregular tachograms) where the ePatch readings were used for the determination of AF. Each subject may have contributed no more than one observation to the analysis of this endpoint.

7.3. Additional Analyses

- Spot tachogram PPV for AF and other arrhythmias
- Alert-level PPV for AF and other arrhythmias
- Sensitivity for AF and specificity for SR for spot tachograms

7.4. Primary Safety Endpoint

The primary safety endpoint is the incidence of serious adverse device effects (ADEs). Adverse device effects are being collected in the ongoing AHS. All serious ADEs reported by participants whose data are included in this sub-study and adjudicated on or before June 22, 2018, were summarized in this CSR.

8. STUDY HYPOTHESIS

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b) (4)

H_0: $PPV_{Tachogram\ (AF)}$ (b) (4)
vs.
H_A: $PPV_{Tachogram\ (AF}$ (b) (4)

There are no hypotheses specified for the secondary efficacy endpoint, additional analyses, or the primary safety endpoint.

9. INVESTIGATIONAL PLAN

9.1. Overall Study Design and Plan

This sub-study used data collected from a subset of participants enrolled in the *Apple Heart Study: Assessment of Wristwatch-Based Photoplethysmography to Identify Cardiac Arrhythmias*, which is a large, prospective, single arm, experimental non-significant risk study, conducted with the assistance of eligible participants without a known history of atrial fibrillation or atrial flutter (at the time of consent). The subjects in this sub-study received an irregular rhythm notification within the AHS App and consequently received and wore an ambulatory ECG patch (ePatch) for interpretation of the ambulatory ECG findings by trained ECG technicians.

All study data were coded with a participant identification (ID). Additional consent was not required to be obtained for this sub-study as this study was determined to be exempt from IRB oversight. The use of the data in this sub-study is consistent with the disclosure of research aims and use of data made to participants in the IRB-approved AHS informed consent.

No additional participation requirements or data, outside of those already required in AHS, were requested of the participants for the purposes of this sub-study analysis.

9.1.1. Study Data Collection Procedures

AHS Study Procedures

Participants in AHS wear their Apple Watch as per normal usage with the AHS App's algorithms analyzing collected PPG pulse data, with two possible outcomes:

1. No irregular heart rhythms consistent with AF that meet the notification threshold are identified from the time monitoring begins (after consenting)

   or;

2. Irregular heart rhythms consistent with AF are identified that meet notification threshold (complete confirmation cycle) during the study. The participant is then notified via the app of this irregularity. Participants who receive a notification during the study will enter the positive notification workflow.

Positive Notification Workflow

The app notification will provide a button for the participant to connect with the Study Telehealth Provider. Upon successful connection, the participant is asked about cardiovascular clinical signs and symptoms. If the Study Telehealth Provider concludes that the participant has a medical emergency, the Study Telehealth Provider will follow its emergency protocol and either instruct the participant and/or a family member, if available, to call emergency medical services (EMS) or will call on the participant's behalf if the participant and/or a family member are unable to contact EMS. These participants will not receive the ambulatory ECG monitors.

Otherwise, if eligible to receive the ePatch, the Study Telehealth Provider will provide the participant information about the ePatch, answer any questions the participant might have, and contact BioTelemetry to initiate the order and shipment of the ePatch.

The BioTelemetry ePatch Monitor will be used for ambulatory ECG monitoring. The battery life with a single channel recording is 7 days. The participant will be instructed to wear the ePatch for up to 7 days. However, the data collected from a participant will be considered adequate for a participant with a minimum analyzable time of 1 hour.

Data Collection and Processing

1. In AHS, eligible participants are sent an ePatch, instructed to wear the patch for up to seven days, and mail the ePatch back to BioTelemetry for processing. BioTelemetry processes the ECG data and generates a standard report for the purposes of the AHS. BioTelemetry also sends raw ECG data to the Sponsor securely for storage. A subset of this data was used for the purposes of this sub-study.

(b) (4)

Data Review

Analysis of ePatch ECG Strips

Two primary, independent adjudicators reviewed each complete ECG strip and provided a diagnosis of the rhythm. The adjudicators classified each of the ECG strips. If there were any differences in the adjudication decisions, the strip in question was sent to a third adjudicator for final decision.

(b) (4)

2. The diagnosis of the rhythm fell into one of four categories:

    i. Sinus Rhythm (SR)
    ii. Atrial Fibrillation (AF)*
    iii. Other Irregular Rhythm (defined below)
    iv. Unreadable (a diagnosis cannot be made as the strip is not adequate for reading)

    *While atrial fibrillation and atrial flutter are two separate conditions, they often manifest similarly in the ECG and can be difficult to differentiate. Clinical treatment of the two conditions is the same. Therefore, for the purposes of this study, the conditions are considered the same.

3. The diagnosis was made via the following logic flow (in sequential order):

(b) (4)

Algorithm Classification

a) The tachogram classification algorithm generated a rhythm classification for a given tachogram, which fell into one of two categories:

   i. Irregular
   ii. Not AF

(b) (4)

The ECG adjudicators were blinded to the tachogram rhythm classifications.

An ECG Adjudication Charter was developed with details of the ECG adjudication process as well as adjudicator qualification criteria and used for adjudicator training purposes.

9.2. Study Population

9.2.1. Inclusion and Exclusion Criteria

In AHS, subjects were required to meet all the following inclusion criteria to be enrolled:

1. Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:
   I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.
   II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.
2. Age ≥ 22 years at time of eligibility screening, ascertained from self-reported date of birth.
3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.
4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.
5. Valid phone number associated with iPhone, ascertained from self-report.
6. Valid email address, ascertained from self-report.

In AHS, subjects who met any of the following criteria were excluded from enrollment:

1. Self-reported diagnosis of atrial fibrillation at time of consent.

2. Self-reported diagnosis of atrial flutter at time of consent.
3. Currently on anticoagulation therapy, as self-reported at the time of consent.

9.2.2. Removal of Subjects from the Study

The sub-study analysis was conducted on a pre-specified group of subjects from the larger AHS. No subjects were removed from the sub-study.

9.2.3. Randomization and Blinding

The design of this sub-study was not randomized.

Independent technologists with extensive and relevant experience reviewed and interpreted the ECG data obtained during the course of the parent AHS. For the purposes of this sub-study, two primary independent adjudicators received (b) strips that corresponded to tachogram time points collected by the Apple Watch. The adjudicators classified each of the ECG strips. If there were any differences in the adjudication decisions, the strip in question was sent to a third adjudicator for final decision.

For the primary endpoint, multiple spot tachograms were generated for each subject during the time of ECG patch wear. (b) (4)

(b) (4)

9.3. Efficacy and Safety Variables

9.3.1. Subject, Spot Tachogram, Alert, and ECG Measurement Accountability

Summary tables which presents subject accountability and spot tachogram, alert, and ECG patch measurement result accountability are reported in **Table 1.1** and **Table 2.2**, respectively.

9.3.2. Demographic and Other Baseline Characteristics

Descriptive statistics (e.g., N, Mean, Std. Dev., Min, Max) for continuous data types and frequencies for categorical data types are displayed for the following demographic and other baseline characteristics in **Table 3**. The following age group categories were used: 22-39, 40-54, 55-64, and 65+:

- Age (Continuous and categorical)
- Sex (Categorical)
- Race (Categorical)
- Height (Continuous)

- Weight (Continuous)
- BMI (Continuous)
- CHA2DS2-VASc score (Continuous)
- Medical History (Categorical)
- Number of cigarettes smoked per day (Categorical)
- Number of alcoholic beverages consumed per week (Categorical)

Subjects may have chosen more than one race category.

9.3.3. Adverse Events

Adverse events were collected through the AHS. All serious adverse device effects (ADEs) reported by participants whose data contributed to this sub-study and were adjudicated on or before June 22, 2018, were considered and analyzed for this sub-study.

9.3.4. Protocol Deviations

Protocol deviations were not captured as part of this sub-study.

9.4. Data Quality Assurance

There was no additional study monitoring for the purposes of the AHS Sub-Study. The data from AHS was monitored in accordance with ICH GCP guidelines.

The Sponsor or designee provided and maintained a charter that describes the independent review and training process for ECG reviewers.

The Sponsor or designee performed internal quality management of data collection, documentation and completion. Quality Control (QC) procedures were implemented beginning with the data entry system (ECG adjudication spreadsheet) and data QC checks that were incorporated into the database (ECG adjudication spreadsheet). Any missing data or data anomalies were communicated to the Sponsor for clarification and resolution.

9.5. Statistical Methods and Determination of Sample Size

9.5.1. Statistical and Analytical Plans

The statistical methods used for the analyses of data are described in the Statistical Analysis Plan (SAP) (Version 3.0, July 26, 2018), which is provided in **Appendix D**. All analyses were performed with SAS, v9.4 or higher and R (b) (4) in a Microsoft Windows environment.

9.5.1.1. Primary Endpoint Analyses

(b) (4) the primary efficacy endpoint of spot tachogram-level PPV for AF was estimated as follows:

$PPV_{Tachogram(AF)}$ = (# of spot tachograms classified as AF according to the spot tachogram algorithm and where the paired ECG strip is classified as AF) / (# of spot tachograms classified as AF according to the spot tachogram algorithm)

A one-sided 97.5% lower confidence bound was computed using an unadjusted normal distribution approximation to the binomial. If the lower bound for the spot tachogram-level PPV exceeded (b) the null hypothesis, H_0, would have been rejected.

(b) (4)

[redacted]

9.5.1.2. Secondary Endpoint Analyses

The alert-level PPV for AF was estimated as follows (b) (4)

[redacted]

$PPV_{Alert(AF)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF) / (# of alert notifications classified as AF according to the alert notification algorithm)

A two-sided exact 95% confidence interval was computed.

(b) (4)

[redacted]

9.5.1.3. Significance Level

The primary hypothesis test of the tachogram-level PPV used a one-sided significance level of 0.025. Two-sided 95% confidence intervals for the secondary and additional analyses are reported.

9.5.1.4. Missing Data/Outliers

Some planned measurements may not have been readable or obtainable. The data analyses were conducted on all readable/classifiable data. No outliers were removed from the analyses after investigation by the Sponsor.

9.5.1.5. Interim Analyses

There were no interim analyses planned in this sub-study.

9.5.1.6. Analysis Sets

All subjects in this sub-study received an AF notification and received an ePatch for ambulatory ECG monitoring. Two analysis sets were pre-defined for this sub-study.

Full Analysis Set (FAS): The Full Analysis Set (FAS) consists of subjects who received an ambulatory ECG monitor and wore their ePatch per the AHS protocol (i.e., were enrolled in this sub-study). Subject accountability, demographic, medical history, and adverse event information are presented for subjects in this analysis set.

ECG Analysis Set (EAS): The ECG Analysis Set (EAS) (b) (4) [redacted] The identification of the subjects to be removed from the EAS were finalized prior to data analysis. All tachogram-level and alert-level outcomes were estimated from this analysis set during times when tachograms and alerts were recorded by Apple Watch during simultaneous, analyzable ECG monitoring.

9.5.1.7. Additional Analyses

For each of the additional endpoint analyses presented below, two-sided 95% confidence intervals are reported using an unadjusted normal distribution approximation to the binomial. A two-sided exact 95% confidence interval are reported for the alert-level PPV for AF and other arrhythmias.

9.5.1.7.1. Spot Tachogram PPV for AF and Other Arrhythmias

The spot tachogram PPV for AF and other arrhythmias were estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) [redacted]

$PPV_{Tachogram(AF\ and\ OA)}$ = (# of spot tachograms classified as AF according to the spot tachogram algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of spot tachograms classified as AF according to the spot tachogram algorithm)

9.5.1.7.2. Alert-Level PPV for AF and Other Arrhythmias

The alert-level (PPV) for AF and Other Arrhythmias were estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) Each subject contributed only one alert notification in this analysis.

$PPV_{Alert\ (AF\ and\ OA)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of alert notifications classified as AF according to the alert notification algorithm).

9.5.1.7.3. Spot Tachogram Sensitivity and Specificity

(b) (4) the spot tachogram sensitivity (for AF) and specificity (for Sinus Rhythm) are calculated and reported along with the corresponding two-sided 95% confidence intervals.

(b) (4)

9.5.2. Determination of Sample Size

The sample size for the primary endpoint of this sub-study is the number of spot tachograms indicating an irregular heart rhythm. (b) (4)

(b) (4)

9.6. Changes in the Conduct of the Study or Planned Analyses

The AHS Sub-Study Protocol (Version 2.0, June 22, 2018) is provided in Appendix C. There were no changes to the study conduct or planned analyses.

10. EFFICACY EVALUATION

10.1. Subject Accountability

Table 1.1 presents the subject accountability in the Full Analysis Set (FAS).

A total of 269 subjects were included in the FAS. Of the 269, 27 subjects were removed from the FAS due to data exclusions and 16 subjects were removed due to lack of ePatch data. Efficacy analyses were performed using the ECG analysis set (EAS) (subjects with ePatch data and tachogram data), which included 226 subjects. Refer to **Listing 8** for the list of subjects excluded from the efficacy analysis.

Table 1.1 Subject Accountability - Full Analysis Set

	Value
Subjects in FAS	269
Subjects Removed from FAS due to Data Exclusions	27
(b) (4) [redacted]	
Subjects in FAS with no Data Exclusions	242
Subjects with no ePatch or Tachogram Data	16
Subjects with ePatch Data and Tachogram Data	226

Data Version: (b) (4) [redacted] (b) (4) [redacted]

10.2. Spot Tachogram, Alert, and ECG Measurement Accountability

Table 2.2 presents spot tachogram, alert, and ECG measurement accountability in the EAS, which included a total of 226 subjects.

The average number of spot tachograms contributed per subject was 46.3 tachograms.

Of the 10,432 total tachograms across all subjects, 25.4% (2650/10432) were classified as 'irregular' and 74.6% (7782/10432) were classified as 'Not AF' by the algorithm. All 10,432 tachograms were reviewed by two primary reviewers; (b) (4) [redacted] 74.8% (169/226) of subjects did not receive any alert during ePatch wear.

Table 2.2 Spot Tachogram, Alert, and ECG Measurement Accountability - EAS

	Value
Number of Subjects in ECG Analysis Set	226
Spot Tachograms Per Subject	
Number of Subjects	226
(b) (4)	[redacted]
Spot Tachogram Classifications	
Irregular	2650 (25.4%)
Not AF	7782 (74.6%)
Total	10432 (100.0%)
Number of Subjects Not Receiving Any Alerts During Patch Wear	169
Number of Subjects Receiving At Least One Alert During Patch Wear	57
(b) (4)	[redacted]

(b) (4)

10.3. Demographic and Other Baseline Characteristics

Table 3 presents demographics and other baseline characteristics for the FAS.

Overall, 80.2% (210/269) of subjects were Male, and 88.8% (239/269) of subjects were White. The mean age of subjects was 59.2 years. Refer to **Listing 2** for details of subject demographics and other baseline characteristics.

Subjects had a mean BMI of 30.3 and mean CHADS-VASC Score of 1.4. Of the 269 subjects, 47.6% (128/269) had history of hypertension, and 1.5% (4/269) had prior history of stroke. Subject medical history listings are provided in **Listing 3.**

Table 3 Demographic and Other Baseline Characteristics – FAS

Characteristic	Subjects (N=269)
Age at Enrollment (years)	
N	268
Mean	59.2
Std. Dev.	13.25
Median	62.0
Min - Max	22 - 89
Age Group [N (%)]	
22-39	27 (10.1%)
40-54	58 (21.6%)
55-64	73 (27.2%)
65+	110 (41.0%)
Sex [N (%)]	
Male	210 (80.2%)
Female	52 (19.8%)
Other	0 (0.0%)
Unknown	0 (0.0%)
Race [N (%)]*	

American Indian	0 (0.0%)
Asian	4 (1.5%)
Black	7 (2.6%)
Hispanic, Latino or Spanish origin	14 (5.2%)
Middle Eastern or North African	2 (0.7%)
Hawaiian or Pacific Islander	0 (0.0%)
White	239 (88.8%)
Other	1 (0.4%)
Prefer not to respond	2 (0.7%)
Height (in)	
N	262
Mean	70.1
Std. Dev.	3.59
Median	70.0
Min - Max	57 - 79
Weight (lbs)	
N	262
Mean	211.8
Std. Dev.	53.88
Median	200.0
Min - Max	120 - 535
Body Mass Index (kg/m2)	
N	262
Mean	30.3
Std. Dev.	7.44
Median	29.0
Min - Max	20 - 79
Medical History [N (%)]*	
Hypertension	128 (47.6%)
Diabetes	43 (16.0%)
Heart Attack	12 (4.5%)
Heart Failure	7 (2.6%)
Stroke	4 (1.5%)
Peripheral Artery Disease	6 (2.2%)
(b) (4) [redacted]	

(b) (4)

10.4. Efficacy Results

10.4.1. Primary Efficacy Endpoint Analysis

Table 4 presents the primary endpoint analysis of spot tachogram PPV for the ECG Analysis Set.

(b) (4)

The spot tachogram PPV analysis resulted in a value of 66.6% (lower confidence bound = 63.0%, p-value 0.9841), which was lower than the pre-specified spot tachogram PPV > 70%.

Refer to **Listing 4** for detailed ePatch adjudication results.

Table 4 Primary Endpoint Analysis of Spot Tachogram PPV - EAS

Parameter	Value	Lower Confidence Bound**	p-value***
(b) (4)			
Spot Tachogram PPV for AF	567/851 (66.6%)	63.0%	0.9841

(b) (4)

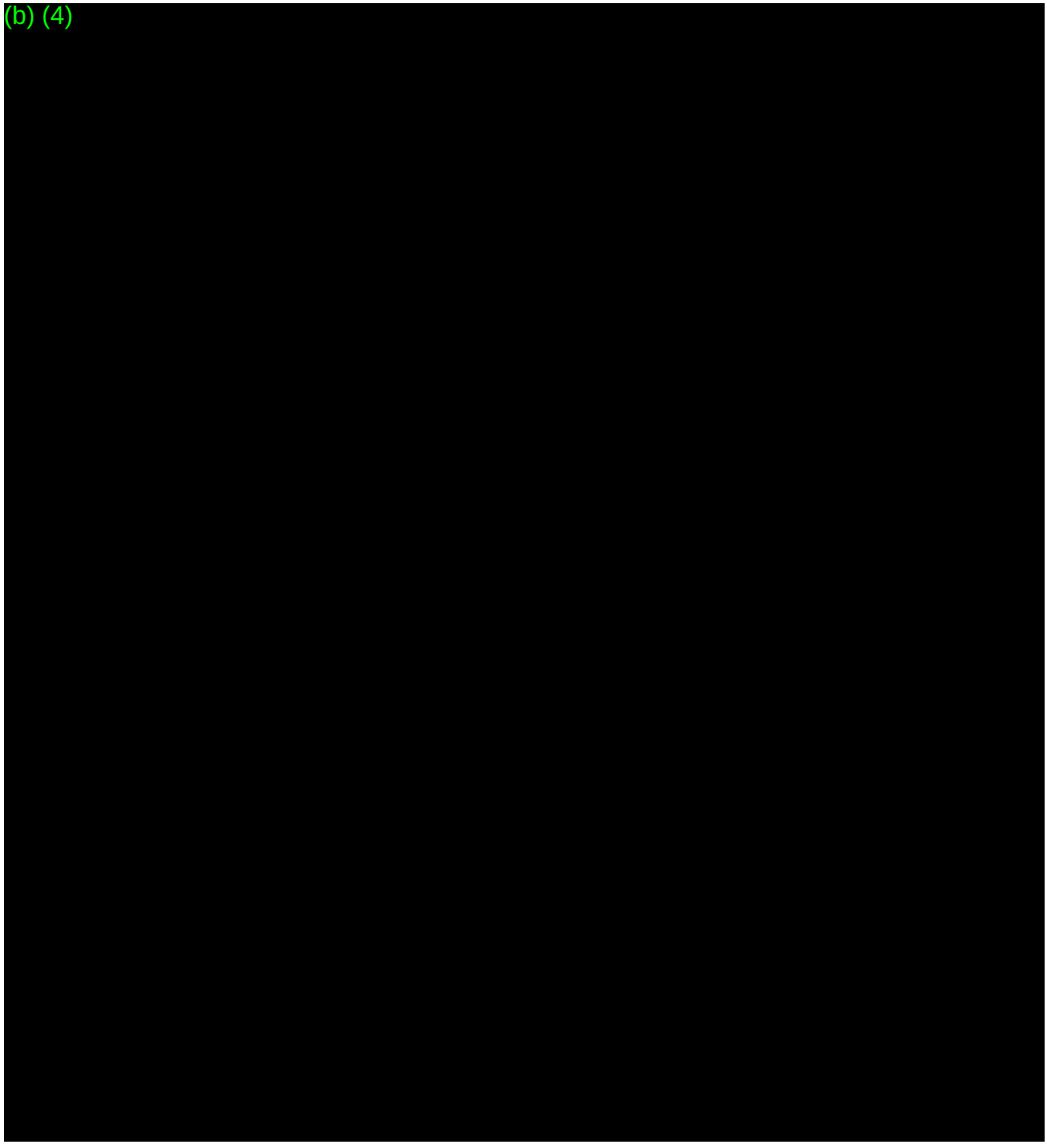
**Lower one-sided 97.5% confidence bound.

***Test of hypothesis for spot tachogram PPV (b)

10.4.2. Primary Efficacy Endpoint Robustness Analyses

(b) (4)

(b) (4)



(b) (4)

[redacted]

10.4.3. Secondary Efficacy Endpoint Analysis

Table 8 presents the secondary endpoint analysis of alert-level PPV for AF in the EAS.

There were 57 subjects with at least one alert-level notification. Of the 57 subjects who received an alert, 45 had at least one tachogram comprising the alert, which corresponded to an ePatch adjudicated result of AF.

The alert-level PPV for AF was 78.9% (45/57) with a two-sided 95% exact confidence interval of (66.1%, 88.6%).

There was no hypothesis associated with the secondary endpoint analysis.

Table 8 Secondary Endpoint Analysis of Alert-Level PPV for AF – EAS

Parameter	Value	Two-Sided 95% Exact Confidence Interval
Number of Subjects with at least 1 alert-level notification*	57	
Alert-level PPV for Atrial Fibrillation/Atrial Flutter	45/57 (78.9%)	(66.1%, 88.6%)
(b) (4) [redacted]		

Note: Numerator for PPV is the number of alerts where at least one of the ePatch results associated with the spot tachograms that comprise the alert is Atrial Fibrillation/Atrial Flutter.

10.4.4. Secondary Efficacy Endpoint Robustness Analyses

Table 9 presents results from the secondary endpoint robustness analysis of alert-level PPV for AF in the EAS using all alerts contributed by the 57 subjects who had at least one alert during ePatch wear. There was one alert where all of the ePatches were deemed Unreadable for all corresponding tachograms comprising the alert per the footnote to the table.

The alert-level PPV from this robustness analysis was 87.0% (322/370) with a two-sided 95% exact confidence interval of (83.5%, 90.3%).

Table 9 Secondary Endpoint Analysis Robustness Analysis of Alert-Level PPV for AF Using All Alerts – EAS

(b) (4)

[redacted]

10.4.5. Additional Analyses

10.4.5.1. Spot Tachogram PPV for AF and Other Arrhythmias

Table 10 presents the spot tachogram PPV for AF and other arrhythmias in the EAS. There were 99 subjects who received at least one irregular tachogram, (b) (4) [redacted] The analysis resulted in a spot tachogram PPV value of 98.4% (837/851) for AF and other arrhythmias.

Table 10 Additional Analysis: Spot Tachogram PPV for AF and Other Arrhythmias - EAS

Parameter	Value	Two-Sided 95% Confidence Interval
Number of subjects with at least 1 irregular spot tachogram	99	
(b) (4) [redacted]		
Spot Tachogram PPV for AF and Other Arrhythmias (b) (4) [redacted]	98.4%)	(97.5%, 99.2%)
(b) (4) [redacted]		

10.4.5.2. Alert-Level PPV for AF and Other Arrhythmias

Table 11 presents the alert-level PPV for AF and other arrhythmias in the EAS.

Across the 57 subjects with at least one alert during ePatch wear, the alert-level PPV for AF and other arrhythmias was 98.2% (56/57).

Table 11 Additional Analysis: Alert-Level PPV for AF and Other Arrhythmias – EAS

Parameter	Value	Two-Sided 95% Exact Confidence Interval
Number of Subjects with at least 1 alert-level notification*	57	
Alert-level PPV for AFib/Atrial Flutter and Other Arrythmias	56/57 (98.2%)	(90.6%, 100.0%)
(b) (4)	(b) (4)	
(b) (4)		

10.4.5.3. Spot Tachogram Sensitivity and Specificity

Table 12 presents the spot tachogram sensitivity and specificity analysis conducted in the EAS.

The sensitivity was 82.9% (b) (4) with a lower confidence interval of 81.4%. The specificity was 99.8% (b) (4) with a lower confidence interval of 99.6%.

Table 12 Additional Analysis: Spot Tachogram Sensitivity and Specificity – EAS

Parameter	Value	Two-Sided Confidence Interval*
(b) (4)		
Sensitivity	(b) (4) (82.9%)	(81.4%, 84.4%)
(b) (4)		
Specificity	(b) (4) (99.8%)	(99.6%, 99.9%)
(b) (4)	(b) (4)	
(b) (4)		

11. SAFETY EVALUATION

11.1. Primary Safety Endpoint Analysis

There were no device-related serious adverse device effects (SADEs) reported in the sub-study.

12. DISCUSSION AND OVERALL CONCLUSIONS

In this sub-study, there were 269 subjects included in the Full Analysis Set (FAS) and 226 subjects in the ECG Analysis Set (EAS). A summary of the results are as follows:

- The primary efficacy endpoint analysis for spot tachogram (b) (4) resulted in a value of **66.6%** (lower confidence bound = 63.0%, p-value 0.9841). This fell below the pre-specified spot tachogram PPV (b) (4)

  (b) (4)

- The secondary efficacy endpoint of alert-level PPV is **78.9%** with a two-sided 95% exact confidence interval of (66.1%, 88.6%) (b) (4)

  (b) (4)

- Additional analyses were conducted with the following results:
  - Spot tachogram PPV for AF and other arrhythmias is **98.4%**.
  - Alert level PPV for AF and Other Arrhythmias is **98.2%**.
  - Spot tachogram sensitivity for AF is **82.9%** and specificity for SR is **99.8%**.
- There were no serious adverse device effects.

13. REFERENCE LIST

[1] Ben Freedman S, Lowres N. Asymptomatic Atrial Fibrillation: The Case for Screening to Prevent Stroke. JAMA. 2015 Nov 10;314(18):1911-2. doi: 10.1001/jama.2015.9846.

[2] Moran PS1, Teljeur C, Ryan M, Smith SM. Systematic screening for the detection of atrial fibrillation. Cochrane Database Syst Rev. 2016 Jun 3;(6):CD009586. doi: 10.1002/14651858.CD009586.pub3.

[3] Lloyd-Jones DM1, Wang TJ, Leip EP, Larson MG, Levy D, Vasan RS, D'Agostino RB, Massaro JM, Beiser A, Wolf PA, Benjamin EJ. Lifetime risk for development of atrial fibrillation: the Framingham Heart Study. Circulation. 2004 Aug 31;110(9):1042-6. Epub 2004 Aug 16.

[4] Colilla S1, Crow A, Petkun W, Singer DE, Simon T, Liu X. Estimates of current and future incidence and prevalence of atrial fibrillation in the U.S. adult population. Am J Cardiol. 2013 Oct 15;112(8):1142-7. doi: 10.1016/j.amjcard.2013.05.063. Epub 2013 Jul 4.

[5] Omboni S1, Verberk WJ2. Opportunistic screening of atrial fibrillation by automatic blood pressure measurement in the community. BMJ Open. 2016 Apr 12;6(4):e010745. doi: 10.1136/bmjopen-2015-010745.

[6] O'Neal WT1, Efird JT2, Judd SE3, McClure LA4, Howard VJ5, Howard G3, Soliman EZ6,7. Impact of Awareness and Patterns of Nonhospitalized Atrial Fibrillation on the Risk of Mortality: The Reasons for Geographic And Racial Differences in Stroke (REGARDS) Study. Clin Cardiol. 2016 Feb;39(2):103-10. doi: 10.1002/clc.22501. Epub 2016 Feb 16.

[7] Brachmann J1, Morillo CA2, Sanna T2, Di Lazzaro V2, Diener HC2, Bernstein RA2, Rymer M2, Ziegler PD2, Liu S2, Passman RS2. Uncovering Atrial Fibrillation Beyond Short-Term Monitoring in Cryptogenic Stroke Patients: Three-Year Results From the Cryptogenic Stroke and Underlying Atrial Fibrillation Trial. Circ Arrhythm Electrophysiol. 2016 Jan;9(1):e003333. doi: 10.1161/CIRCEP.115.003333.

[8] Evaluation and Reporting of Age-, Race-, and Ethnicity-Specific Data in Medical Device Clinical Studies. FDA Guidance Document. September 12, 2017.

Appendix A. Signature Page

Protocol Title: Apple Heart Study Sub-Study
Protocol Date: June 22, 2018
Protocol Version: 2.0

I confirm that I have read and attest to the accuracy of the Apple Heart Study Sub-Study Clinical Study Report, dated August 7, 2018.

(b) (6)

[redacted]

Printed Name/Title Signature Date

Appendix B. IRB Information

Using the Department of Health and Human Services regulations found at 45 CFR 46.101(b)(4), the Institutional Review Board (IRB) determined that the Apple Heart Study (AHS) Sub-Study is exempt from IRB oversight. Documentation of IRB exempt status was obtained.

IRB Contact Information:

(b) (4)

Apple Heart Study Sub-Study Protocol
APN: 099-14037-A, ECO 0013154195

Sponsor:	**Apple, Inc.**
Version and date:	**Version 2.0, June 22, 2018**
Compliance Statement:	This study will be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, clinical research guidelines established by the U.S. Food and Drug Administration (21 CFR Parts 50, 54, 56, and 812), and ICH GCP Guidelines.

Version	Date	Significant Revisions
1.0	April 26, 2018	A (Initial Version)
2.0	June 22, 2018	Updated data-cut date; Clarification on subject confidentiality; (b) (4) sample size, analysis set, and statistical analysis plan

PROTOCOL SYNOPSIS

Apple Heart Study Sub-Study Protocol

Overview

This Apple Heart Study Sub-Study (AHS Sub-Study) Protocol describes the analysis that will be conducted on a subset of data from the ongoing Apple Heart Study. This AHS Sub-Study is being conducted to determine if the tachogram classification algorithm and confirmation cycle algorithm (alert-level) have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF) in a subset of AHS participants.

Study Objective

The objective of this AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF).

Study Endpoints

- Primary Endpoint: Identification of irregular rhythm consistent with AF as suggested by positive predictive value (PPV) of the spot tachogram [Spot Tachogram PPV]
- Secondary Endpoint: Identification of irregular rhythm consistent with AF as suggested by PPV of the notification [Alert-Level PPV]
- Primary Safety Endpoint: Serious adverse device effects (ADEs)

Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b)

H0: $PPV_{Tachogram(AF)}$ (b)

vs.

HA: $PPV_{Tachogram(AF)}$ (b)

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

Subject Population

AHS began on November 30, 2017. The data to support this sub-study will come from AHS participants who were enrolled between November 30, 2017, to approximately June 22, 2018, who have received the ECG patch (ePatch provided by BioTelemetry) and for whom ECG data has been adjudicated. The analysis defined in this sub-study protocol will not be initiated until all participant data (up to June 22, 2018) to be used in the analysis is available.

To ensure the confidentiality of the subject data, subject data will be identified by a participant ID number for which the Sponsor will not have the ability to link back to the subject's identity. The use of the data in this sub-study is consistent with the disclosure of research aims and use of the data made to the subjects in the IRB-approved Apple Heart Study informed consent form.

The inclusion/exclusion criteria for the AHS is as follows:

Inclusion Criteria

Subjects must meet all the following inclusion criteria to be enrolled:

- Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:

    I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.

    II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.

2. Age ≥ 22 years at time of eligibility screening, ascertained from self-reported date of birth.

3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.

4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.

5. Valid phone number associated with iPhone, ascertained from self-report.

6. Valid email address, ascertained from self-report.

Exclusion Criteria

Subjects who meet any of the following criteria may not be enrolled:

1. Self-reported diagnosis of Atrial Fibrillation at time of consent.

2. Self-reported diagnosis of Atrial Flutter at time of consent.

Currently on anticoagulation therapy, as self-reported at the time of consent.

Sample Size

The sample size in this sub-study is the number of spot tachograms. (b) (4) [redacted]

(b) (4) [redacted]

LIST OF ABBREVIATIONS

The following abbreviations are used in this study protocol.

Abbreviation or Specialist Term	Explanation
ADE	Adverse Device Effect
AF	Atrial Fibrillation
AHS	Apple Heart Study
CFR	Code of Federal Regulations
EAS	ECG Analysis Set
ECG	Electrocardiogram
FDA	Food and Drug Administration
GCP	Good Clinical Practice
ICF	Informed Consent Form
ICH	International Conference on Harmonisation
IPNA	Irregular Pulse Notification Algorithm
IRB	Institutional Review Board
SR	Sinus Rhythm
PPG	Photoplethysmogram
QC	Quality Control

1. INTRODUCTION

Background

AF is the most common serious cardiac arrhythmia, and, when left untreated, is a leading cause of morbidity and mortality from stroke, heart failure and myocardial infarction[1,2]. Data from the Framingham Heart Study indicates that by age 40 years, lifetime risk for developing AF is 1 in 4[3]. AF is also a growing public health problem with prevalence projected to triple between 2010 and 2050, with an estimated 12.1 million diagnosed cases in 2030 in the United States alone[4].

Early detection and treatment of patients with AF minimizes the risk of sequelae of thromboembolism including >60% reduced risk of stroke[2,5]. However, many affected with AF are unaware they have this arrhythmia due to a number of factors, including lack of symptoms, or they may experience only mild symptoms that they do not attribute to a disease[2]. As a result, asymptomatic patients are 3 times as likely to have sustained an ischemic stroke prior to diagnosis than those with symptoms[1,6]. These findings raise concerns and have prompted several variations of screening programs to detect patients with asymptomatic AF to prevent an embolic event[1,2]. While systematic and opportunistic screening programs have demonstrated increased rates of detection when compared to detection during routine clinical practice, such screening programs are not yet widely implemented[2]. Additionally, AF may be paroxysmal (PAF, or intermittent AF) and therefore missed by recording a single in-clinic electrocardiogram (ECG). This is especially true for those patients with intermittent symptoms. Holter devices are commonly used for ambulatory 24-hour ECG monitoring in at-risk patients, but have limited sensitivity for the detection of new AF[7].

Overview of the Apple Heart Study (AHS) Protocol

The AHS is an app-based research study being conducted through the AHS app. As in other mobile-mediated research studies, the informed consent process in the AHS is conducted remotely in a completely self-administered setting with no required contact with the research team prior to consent and enrollment.

The potential participant first downloads the AHS app. The app automatically ensures compatibility with the iPhone iOS version and Watch version. If compatible, the participant is able to continue forward in the app. An overview of the study is displayed in the app.

The participant advances to a screen for study enrollment, where they confirm whether they meet general participation requirements. The participant is asked questions based on study inclusion and exclusion criteria. The app automatically determines eligibility based on the responses provided. If the participant is determined to be eligible, they are presented with an in-app consent and authorization form to be read and signed if they agree to participate.

A copy of the signed study consent and authorization document is available for review and download to the participant via the app. After consenting to participate, the participant is directed to complete a brief questionnaire to collect self-reported baseline demographics and

medical history. The participant is considered 'enrolled' from this point and the study app's analysis of Apple Watch photoplethysmogram (PPG) sensor data begins thereafter.

The approach to informed consent for the AHS is meant to ensure that participants are adequately informed about the research before agreeing to participate. Potential candidates as well as enrolled participants are able to contact an AHS hotline (available 24/7 at 1-844-606-1609) any time and have the ability to ask questions, request clarifications, or report a problem at any time prior to or during the study. This hotline is open from the study start date until study closure.

If the participant receives an irregular rhythm notification, they are instructed to connect with a Study Telehealth Provider and, if the participant is eligible, receives an ambulatory ECG monitor (ePatch) to wear while the study app is analyzing Apple Watch PPG sensor data.

Study Device Description

The AHS app is a mobile medical application used in the AHS. Because the study is being conducted completely virtually, the app functions as a means to screen for inclusion/exclusion criteria, collect the electronic informed consent, collect user information and medical history, and is used by the subjects to connect to a study telehealth provider if they receive an irregular rhythm notification or if they need to report a problem (described in section above). The app also contains the tachogram classification algorithm and alert-level confirmation cycle algorithm, both of which are being validated in this sub-study.

The tachogram classification algorithm classifies a tachogram as irregular or not AF, and the alert-level confirmation cycle algorithm determines if a notification will be surfaced to the user. At baseline, the Apple Watch platform will attempt to capture a tachogram every 2–4 hours to support the commercially available HRV feature, and the AHS App will retrieve and analyze any such tachograms that are captured. If a tachogram is classified as irregular, the "confirmation cycle" begins, during which the AHS App requests additional tachograms from the platform more frequently (as frequently as possible subject to a minimum spacing of 15 minutes). If five out of six sequential tachograms (including the initial one) are classified as irregular within a 48-hour period, a notification of this finding is surfaced to the user. If two tachograms are classified as not AF before this threshold is reached, the AHS App returns to baseline (attempting to retrieve tachograms every 2-4 hours), no results are surfaced, and the confirmation cycle is reset (that is, any irregular tachograms within this sequence do not count in future confirmation cycles).

The AHS App will surface the first notification to the user, which initiates the workflow to call the study telehealth provider and receive the ePatch. After the first notification is surfaced, no additional notifications will be surfaced to the user. However, notifications will continue to be generated for the purposes of data analysis ("silent notifications"). The classified tachograms that contribute to a notification and the notification itself will be stored and used for the alert-level PPV analysis.

The tachogram and notification data being collected and processed through the algorithms within the AHS App are the subject of this sub-study, and will be compared to the gold-standard ECG to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV. Apple intends to leverage this data to support clearance of the (b) (4) App which incorporates the same algorithms as those being validated through this sub-study.

AHS Study Procedures

Participants in AHS wear their Apple Watch as per normal usage with the AHS App's algorithms analyzing collected PPG pulse data, with two possible outcomes:

1. No irregular heart rhythms consistent with AF that meet the notification threshold are identified from the time monitoring begins (after consenting)

   or;

2. Irregular heart rhythms consistent with AF are identified that meet notification threshold (complete confirmation cycle) during the study. The participant is then notified via the app of this irregularity. Participants who receive a notification during the study will enter the positive notification workflow.

Positive Notification Workflow

The app notification will provide a button for the participant to connect with the Study Telehealth Provider. Upon successful connection, the participant is asked about cardiovascular clinical signs and symptoms. If the Study Telehealth Provider concludes that the participant has a medical emergency, the Study Telehealth Provider will follow its emergency protocol and either instruct the participant and/or a family member, if available, to call emergency medical services (EMS) or will call on the participant's behalf if the participant and/or a family member are unable to contact EMS. These participants will not receive the ambulatory ECG monitors.

Otherwise, if eligible to receive the ePatch, the Study Telehealth Provider will provide the participant information about the ePatch, answer any questions the participant might have, and contact BioTelemetry to initiate the order and shipment of the ePatch.

The BioTelemetry ePatch Monitor will be used for ambulatory ECG monitoring. The battery life with a single channel recording is 7 days. The participant will be instructed to wear the ePatch for up to 7 days. However, the data collected from a participant will be considered adequate for a participant with a minimum analyzable time of 1 hour.

Study Rationale

AHS is a research study initiated to understand the true prevalence of undiagnosed atrial fibrillation (AF) in a large population in order to better understand the utility of this diagnosis in the asymptomatic population, and to notify those who did not know they have AF of its presence and potential risk of stroke.

The purpose of the AHS Sub-Study is to conduct an analysis on a pre-specified subset of data collected in AHS to support a regulatory submission before the AHS ends. Individual tachograms

taken from a user's watch at the same time they are wearing the ePatch as well as silent notifications that occur during patch wear will be used to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV.

Risk/Benefit Assessment

No significant risks or permanent side effects are anticipated as this sub-study is intended to leverage data already being collected in the AHS. All study data will be coded with a participant ID. The use of the data in this sub-study is consistent with the disclosure of research aims and use of data made to participants in the IRB-approved AHS informed consent.

2. STUDY OBJECTIVES, ENDPOINTS, AND HYPOTHESIS

Study Objective

The objective of this AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF).

Study Endpoints

- Primary Efficacy Endpoint: Identification of irregular rhythm consistent with AF as suggested by positive predictive value (PPV) of the spot tachogram [Spot Tachogram PPV] where the ECG patch readings (paired to the timestamp associated with the spot tachograms) are used for the determination of AF.
- Secondary Efficacy Endpoint: Identification of irregular rhythm consistent with AF as suggested by PPV of the alert [Alert-Level PPV] (based on multiple irregular tachograms) where the ECG patch readings are used for the determination of AF.
- Primary Safety Endpoint: Incidence of serious adverse device effects (ADEs).

Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b)

H0: $PPV_{Tachogram(AF)}$ (b)

vs.

HA: $PPV_{Tachogram(AF)}$ (b)

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

3. SUB-STUDY DESIGN

Overview

The purpose of the AHS Sub-Study is to conduct an analysis on a pre-specified subset of data collected in AHS to support a regulatory submission before the AHS ends. Individual tachograms taken from a user's watch at the same time they are wearing the ePatch as well as silent notifications that occur during patch wear will be used to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV.

All study data will be coded with a participant ID. The use of the data in this sub-study is consistent with the disclosure of research aims and use of data made to participants in the IRB-approved AHS informed consent.

Duration of Subject Participation

No additional participation requirements or data, outside of those already required in AHS, will be requested of the participants for the purposes of this sub-study analysis.

4. STUDY POPULATION

Subject Population

AHS began on November 30, 2017. The data to support this sub-study will come from AHS participants who were enrolled between November 30, 2017, to approximately June 22, 2018, who have received the ECG patch (ePatch provided by BioTelemetry) and for whom patch data has been adjudicated.

To ensure the confidentiality of the subject data, subject data will be identified by a participant ID number for which the Sponsor will not have the ability to link back to the subject's identity. The use of the data in this sub-study is consistent with the disclosure of research aims and use of the data made to the subjects in the IRB-approved Apple Heart Study informed consent form.

The inclusion/exclusion criteria for the AHS is as follows:

Inclusion Criteria

Subjects must meet all the following inclusion criteria to be enrolled:

1. Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:

    I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.

    II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.

2. Age $\geq$ 22 years at time of eligibility screening, ascertained from self-reported date of birth.

3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.

4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.

5. Valid phone number associated with iPhone, ascertained from self-report.

6. Valid email address, ascertained from self-report.

Exclusion Criteria

Subjects who meet any of the following criteria may not be enrolled:

1. Self-reported diagnosis of Atrial Fibrillation at time of consent.
2. Self-reported diagnosis of Atrial Flutter at time of consent.
3. Currently on anticoagulation therapy, as self-reported at the time of consent.

Subject Follow up

No additional follow-up or participation requirements are requested of the participants outside those in the AHS.

5. SUB-STUDY PROCEDURES

Data collection and processing

1. In AHS, eligible participants are sent an ePatch, instructed to wear the patch for up to seven days, and mail the ePatch back to BioTelemetry for processing. BioTelemetry processes the ECG data and generates a standard report for the purposes of the AHS. BioTelemetry also sends raw ECG data to Apple securely for storage. A subset of this data will be used for the purposes of this sub-study.

(b) (4)

[redacted]

Data Review

Analysis of reference strips

- Two blinded independent adjudicators will review each complete ECG strip and provide a diagnosis of the rhythm.

(b) (4)

- The diagnosis of the rhythm will fall into one of four categories:

  i. Sinus rhythm (SR)

  ii. Atrial fibrillation (AF)*

  iii. Other Irregular Rhythm (defined below)

  iv. Unreadable (a diagnosis cannot be made as the strip is not adequate for reading)

- The diagnosis will be made via the following logic flow (in sequential order):

(b) (4)

(b) (4)

Algorithm classification

a) The tachogram classification algorithm will generate a rhythm classification for a given tachogram , which will fall into one of two categories:

   i. Irregular

   ii. Not AF

(b) (4)

The BioTelemetry ECG adjudicators will be blinded to the tachogram rhythm classifications.

An ECG Adjudication Charter will be developed with details of the ECG adjudication process as well as adjudicator qualification criteria and used for adjudicator training purposes.

*While atrial fibrillation and atrial flutter are two separate conditions, they often manifest similarly in the ECG and can be difficult to differentiate. Clinical treatment of the two conditions is the same. Therefore, for the purposes of this study, the conditions will be considered the same.

6. STATISTICAL ANALYSIS

6.1 Study Endpoints

6.1.1 Primary Efficacy Endpoint

The primary efficacy endpoint of this study is the identification of irregular rhythm consistent with AF as suggested by positive predictive value of the spot tachogram where the ECG patch readings (paired to the timestamp associated with the spot tachograms) are used for the determination of AF. Each subject may contribute multiple observations (i.e., spot tachograms) for this endpoint.

6.1.2 Secondary Efficacy Endpoint

The secondary efficacy endpoint is the identification of irregular rhythm consistent with AF as suggested by positive predictive value of the alert (based on multiple irregular tachograms) where the ECG patch readings are used for the determination of AF. Each subject may contribute no more than one observation to the analysis of this endpoint.

6.1.3 Additional Analyses

- Spot Tachogram PPV for AF and other arrhythmias
- Alert-level PPV for AF and other arrhythmias
- Sensitivity and specificity for spot tachograms

6.1.4 Primary Safety Endpoint

The primary safety endpoint is the incidence of serious adverse device effects (ADEs). Adverse device effects are being collected through the AHS. All serious ADEs reported by participants whose data will contribute to this sub-study and adjudicated on or before approximately June 22, 2018, will be considered and analyzed for submission.

6.2 Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least 0.70:

H0: $PPV_{Tachogram(AF)} < 0.70$

vs.

HA: $PPV_{Tachogram(AF)} > 0.70$

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

6.3 Statistical Considerations

6.3.1 Sample Size

The sample size for the primary endpoint of this sub-study is the number of spot tachograms indicating an irregular heart rhythm. (b) (4)

[redacted]

(b) (4)

6.3.2 Randomization and Blinding

The design of this sub-study is not randomized. Independent technologists with extensive and relevant experience will review and interpret the ECG data obtained during the course of the parent Apple Heart Study. For the purposes of this sub-study, two primary independent adjudicators will receive (b) strips that correspond to tachogram time points collected by the Apple Watch. The adjudicators will classify each of the ECG strips. If there are any differences in the adjudication decisions, the strip in question will be sent to a third adjudicator for final decision.

For the primary endpoint, multiple spot tachograms will be generated for each subject during the time of ECG patch wear. (b) (4)

(b) (4)

6.3.3 Significance Level

The primary hypothesis test of the tachogram-level PPV will use a one-sided significance level of 0.025. Two-sided 95% confidence intervals for the secondary and tertiary endpoints will be reported.

6.3.4 Missing Data/Outliers

Rigorous efforts will be made to ensure all subjects are compliant with the protocol. However, some subjects may drop out prematurely or some planned measurements may not be readable or obtainable. The data analyses will be conducted on all readable/classifiable data. Outliers may be removed from the analyses after investigation by the sponsor and biostatistician.

6.3.5 Interim Analyses

There are no interim analyses planned in this sub-study.

6.3.6 Analysis Sets

All subjects in this sub-study will have received an AF notification and will have received a patch for ambulatory ECG monitoring. Therefore, only one analysis set is defined for this sub-study.

ECG Analysis Set (EAS): The ECG Analysis Set (EAS) will consist of subjects who receive an ambulatory ECG monitor and wear their ePatch per the AHS protocol. All tachogram-level and alert-level outcomes will be estimated from this analysis set during times when tachograms and alerts are being recorded by Apple Watch during simultaneous, analyzable ECG monitoring.

6.3.7 Statistical Software

All analyses will be performed with SAS, v9.4 or higher and R (b) (4) in a Microsoft Windows environment.

7. SAFETY PARAMETERS AND ASSESSMENT

Adverse Events

Adverse events are being collected through the AHS. All serious adverse device effects (ADEs) reported by participants whose data will contribute to this sub-study and adjudicated on or before approximately June 22, 2018, will be considered and analyzed for submission.

8. REGULATORY, ETHICAL, AND STUDY OVERSIGHT CONSIDERATIONS

Institutional Review Board

Good Clinical Practice (GCP) requires that the clinical protocol, any protocol amendments, informed consent, and all other forms of subject- and reviewer-related materials be reviewed by an IRB. IRB approval of the protocol, informed consent and subject information and/or advertising was obtained for the AHS prior to study initiation.

Informed Consent

Informed consent was obtained from all AHS participants from whom data is being used to support data analysis for the AHS Sub-Study. Study participants were informed that their study data could be used in the context of a regulatory submission and for commercial purposes.

Ethical Conduct of Study

This study will be conducted in accordance with GCP guidelines. Trial documents should be retained until at least 2 years after the last approval of marketing application in an ICH region and until there are no pending or contemplated-marketing applications in an ICH region. If there are no local laws, sites should retain filed for 5 years after completion of the study.

Confidentiality and Privacy

Subject confidentiality is strictly held in trust by the participating investigators, their staff, and the Sponsor and its agents. The study protocol, documentation, data and all other information generated will be held in strict confidence. No information concerning the study or the data will be released to any unauthorized third party without prior written approval of the Sponsor. Only password-protected, coded study data (using Participant ID) will be sent to the BioTelemetry Adjudication Committee for review.

Data Collection and Management Responsibilities

A subset of the data collected in the AHS will be used in the AHS Sub-Study. The Sponsor or designee will supply the case report forms (CRFs) in the form of a spreadsheet to the Adjudication Committee for additional review.

The Sponsor may permit trial-related monitoring, audits, IRB review and regulatory inspections(s), providing access to data documents.

Study Monitoring

There is no additional study monitoring for the purposes of the AHS Sub-Study. The data from AHS has been monitored in accordance with ICH GCP guidelines. The Investigators have

monitored adherence to the study protocol and the completeness, consistency, and accuracy of data collected in AHS.

Data Quality Assurance and Quality Control

The Sponsor or designee will provide and maintain a charter that describes the independent review and training process for reviewers.

The Sponsor or designee will perform internal quality management of data collection, documentation and completion. Quality Control (QC) procedures will be implemented beginning with the data entry system (spreadsheet) and data QC checks that will be incorporated into the database (spreadsheet). Any missing data or data anomalies will be communicated to the Sponsor for clarification/resolution.

Use of Information

All information concerning the AHS Sub-Study is considered confidential information. The information developed during the conduct of the AHS is also considered confidential and will be used by the Sponsor in connection with the development of the algorithm.

Study Termination

The Sponsor reserves the right to terminate the AHS Sub-Study at any time. In terminating the AHS Sub-Study, the Sponsor will assure that adequate consideration is given to the protection of the participants' interests.

Completion of the Study

The Sponsor agrees to complete this study in satisfactory compliance with the protocol and all applicable regulatory requirements.

REFERENCES

[1] Ben Freedman S, Lowres N. Asymptomatic Atrial Fibrillation: The Case for Screening to Prevent Stroke. JAMA. 2015 Nov 10;314(18):1911-2. doi: 10.1001/jama.2015.9846.

[2] Moran PS1, Teljeur C, Ryan M, Smith SM. Systematic screening for the detection of atrial fibrillation. Cochrane Database Syst Rev. 2016 Jun 3;(6):CD009586. doi: 10.1002/14651858.CD009586.pub3.

[3] Lloyd-Jones DM1, Wang TJ, Leip EP, Larson MG, Levy D, Vasan RS, D'Agostino RB, Massaro JM, Beiser A, Wolf PA, Benjamin EJ. Lifetime risk for development of atrial fibrillation: the Framingham Heart Study. Circulation. 2004 Aug 31;110(9):1042-6. Epub 2004 Aug 16.

[4] Colilla S1, Crow A, Petkun W, Singer DE, Simon T, Liu X. Estimates of current and future incidence and prevalence of atrial fibrillation in the U.S. adult population. Am J Cardiol. 2013 Oct 15;112(8):1142-7. doi: 10.1016/j.amjcard.2013.05.063. Epub 2013 Jul 4.

[5] Omboni S1, Verberk WJ2. Opportunistic screening of atrial fibrillation by automatic blood pressure measurement in the community. BMJ Open. 2016 Apr 12;6(4):e010745. doi: 10.1136/bmjopen-2015-010745.

[6] O'Neal WT1, Efird JT2, Judd SE3, McClure LA4, Howard VJ5, Howard G3, Soliman EZ6,7. Impact of Awareness and Patterns of Nonhospitalized Atrial Fibrillation on the Risk of Mortality: The Reasons for Geographic And Racial Differences in Stroke (REGARDS) Study. Clin Cardiol. 2016 Feb;39(2):103-10. doi: 10.1002/clc.22501. Epub 2016 Feb 16.

[7] Brachmann J1, Morillo CA2, Sanna T2, Di Lazzaro V2, Diener HC2, Bernstein RA2, Rymer M2, Ziegler PD2, Liu S2, Passman RS2. Uncovering Atrial Fibrillation Beyond Short-Term Monitoring in Cryptogenic Stroke Patients: Three-Year Results From the Cryptogenic Stroke and Underlying Atrial Fibrillation Trial. Circ Arrhythm Electrophysiol. 2016 Jan;9(1):e003333. doi: 10.1161/CIRCEP.115.003333.

STATISTICAL ANALYSIS PLAN

APPLE HEART STUDY SUB-STUDY
APN: 099-14038-A, ECO 0013154195

For:

Apple Inc.
1 Apple Park Way
Cupertino, CA 95014
United States

By:
(b) (4)
Lead Biostatistician

Initial Version Date:	April 26, 2018
Current Version Number:	Version 3
Current Version Date:	July 26, 2018

Table of Contents

Statistical Analysis Plan Approval Signature Page

The undersigned have reviewed and approve the Statistical Analysis Plan.

SIGNATURES

Sponsor Signatory	**Signature**	**Date**
Name/Title	(b) (6) [redacted] PhD/Lead Biostatistician	26 Jul 2018
Name/Title		
Name/Title		

LIST OF ABBREVIATIONS

ADE	Adverse Device Effect
AF	Atrial Fibrillation or Atrial Flutter
AHS	Apple Heart Study
EAS	ECG Analysis Set
ECG	Electrocardiogram
FAS	Full Analysis Set
GEE	Generalized Estimating Equations
OA	Other Arrhythmias
PPG	Photoplethysmogram
PPV	Positive Predictive Value
SR	Sinus Rhythm
Std. Dev	Standard Deviation

1. Version History

Version (Date)	Summary of Changes	Author(s)/Title
v1 (26APR2018)	Initial Version	(b) (6) /Lead Biostatistician
v2 (22Jun2018)	Added CHA2DS2-VASc score analysis, added sensitivity and specificity analyses for the tachograms, and added additional robustness analyses for tachogram and alert-level PPV.	(b) (6) /Lead Biostatistician
v3 (25Jul2018)	Added Per Protocol Analysis Set	(b) (6) /Lead Biostatistician

2. Introduction

This statistical analysis plan describes the analysis of the Apple Heart Study (AHS) Sub-Study.

2.1. Background

The AHS app is a mobile medical application used in the AHS. The App contains the tachogram classification algorithm and alert-level confirmation cycle algorithm, both of which are being validated in this sub-study. The tachogram classification algorithm classifies a tachogram as irregular or not AF, and the alert-level confirmation cycle algorithm determines if a notification will be surfaced to the user. At baseline, the Apple Watch platform will attempt to capture a tachogram every 2–4 hours and the AHS App will retrieve and analyze any such tachograms that are captured. When the AHS App retrieves a tachogram, it assesses the degree and pattern of variability to classify it as irregular or not AF. The tachogram classification algorithm then sends classified tachograms to the confirmation cycle algorithm, during which the AHS App requests additional tachograms from the platform more frequently (as frequently as possible subject to a minimum spacing of 15 minutes). If five out of six sequential tachograms (including the initial one) are classified as irregular within a 48-hour period, a notification of this finding is surfaced to the user. If two tachograms are classified as not AF before this threshold is reached, the AHS App returns to baseline (attempting to retrieve tachograms every 2-4 hours), no results are surfaced, and the confirmation cycle is reset (that is, any irregular tachograms within this sequence do not count in future confirmation cycles).

2.2. Study Rationale

AHS is a research study initiated to understand the true prevalence of undiagnosed atrial fibrillation (AF) in a large population in order to better understand the utility of this diagnosis in the asymptomatic population, and to notify those who did not know they have AF of its presence and potential risk of stroke.

The purpose of the AHS Sub-Study is to conduct an analysis on a pre-specified subset of data collected in AHS to support a regulatory submission before the AHS ends. Individual tachograms taken from a user's watch at the same time they are wearing the ePatch as well as silent notifications that occur during patch wear will be used to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV.

3. Study Objective

The objective of this AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF).

4. Study Design

This sub-study will use data collected from a subset of participants enrolled in the *Apple Heart Study: Assessment of Wristwatch-Based Photoplethysmography to Identify Cardiac Arrhythmias*, which is a large, prospective, single arm, experimental non-significant risk study, conducted with the assistance of eligible participants without a known history of atrial fibrillation or atrial flutter (at the time of consent). The subjects in this sub-study will have received an irregular rhythm notification within the Apple Heart Study App and consequently have received and worn an ambulatory electrocardiographic (ECG) patch for interpretation of the ambulatory ECG findings by trained ECG technicians. No additional participation requirements or data, outside of those already required in AHS, will be requested of the subjects for the purposes of this sub-study analysis.

5. Study Endpoints

5.1. Primary Efficacy Endpoint

The primary efficacy endpoint of this study is the identification of irregular rhythm consistent with AF as suggested by positive predictive value of the spot tachogram where the ECG patch readings (paired to the timestamp associated with the spot tachograms) are

used for the determination of AF. Each subject may contribute multiple observations (i.e., spot tachograms) for this endpoint.

5.2. Secondary Efficacy Endpoint

The secondary efficacy endpoint is the identification of irregular rhythm consistent with AF as suggested by positive predictive value of the alert (based on multiple irregular tachograms) where the ECG patch readings are used for the determination of AF. Each subject may contribute no more than one observation to the analysis of this endpoint.

5.3. Additional Analyses

- Spot Tachogram PPV for AF and other arrhythmias (defined in the protocol)
- Alert-level PPV for AF and other arrhythmias (defined in the protocol)Sensitivity and specificity for spot tachograms

5.4. Primary Safety Endpoint

The primary safety endpoint is the incidence of serious adverse device effects (ADEs). Adverse device effects are being collected through the AHS. All serious ADEs reported by participants whose data will contribute to this sub-study and adjudicated on or before approximately June 22, 2018, will be considered and analyzed for submission.

6. Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b)

H_0: $PPV_{Tachogram(AF)}$ (b)
vs.
H_A: $PPV_{Tachogram(AF)}$ (b)

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

7. Statistical Considerations

7.1. Sample Size

The sample size for the primary endpoint of this sub-study is the number of spot tachograms indicating an irregular heart rhythm. (b) (4)

[redacted]

(b) (4)

[redacted]

7.2. Randomization and Blinding

The design of this sub-study is not randomized. Independent technologists with extensive and relevant experience will review and interpret the ECG data obtained during the course of the parent Apple Heart Study. For the purposes of this sub-study, two primary independent adjudicators will receive (b) strips that correspond to tachogram time points collected by the Apple Watch. The adjudicators will classify each of the ECG strips. If there are any differences in the adjudication decisions, the strip in question will be sent to a third adjudicator for final decision.

For the primary endpoint, multiple spot tachograms will be generated for each subject during the time of ECG patch wear. (b) (4)

[redacted]

(b) (4)

[redacted]

7.3. Significance Level

The primary hypothesis test of the tachogram-level PPV will use a one-sided significance level of 0.025. Two-sided 95% confidence intervals for the secondary and tertiary endpoints will be reported.

7.4. Missing Data/Outliers

Rigorous efforts will be made to ensure all subjects are compliant with the protocol. However, some subjects may drop out prematurely or some planned measurements may not be readable or obtainable. The data analyses will be conducted on all readable/classifiable data. Outliers may be removed from the analyses after investigation by the sponsor and biostatistician.

7.5. Interim Analyses

There are no interim analyses planned in this sub-study.

8. Analysis Sets

All subjects in this sub-study will have received an AF notification and will have received a patch for ambulatory ECG monitoring. Two analysis sets are defined for this sub-study.

Full Analysis Set (FAS): The Full Analysis Set (FAS) will consist of subjects who receive an ambulatory ECG monitor and wear their ePatch per the AHS protocol (i.e., were enrolled in this sub-study). Subject accountability, demographic, medical history, and adverse event information will be presented for subjects in this analysis set.

ECG Analysis Set (EAS): (b) (4) [redacted] The identification of the subjects to be removed from the EAS will be finalized prior to data analysis. All tachogram-level and alert-level outcomes will be estimated from this analysis set during times when tachograms and alerts are being recorded by Apple Watch during simultaneous, analyzable ECG monitoring.

9. Analysis Approach

9.1. Subject, Spot Tachogram, Alert, and ECG Measurement Accountability

Summary tables will be reported which present the accountability of subjects (FAS) and accountability of spot tachograms, alerts, and ECG patch measurement results (EAS).

9.2. Demographic and Other Baseline Characteristics

Descriptive statistics (e.g., N, Mean, Std. Dev., Min, Max) for continuous data types and frequencies for categorical data types will be displayed for the following demographic and other baseline characteristics. The following age group categories will be used: 22-39, 40-54, 55-64, and 65+:

- Age (Continuous and categorical)
- Sex (Categorical)
- Race (Categorical)

- Height (Continuous)
- Weight (Continuous)
- BMI (Continuous)
- CHA_2DS_2-VASc score (Continuous)
- Medical History (Categorical)
- Number of cigarettes smoked per day (Categorical)
- Number of alcoholic beverages consumed per week (Categorical)

9.3. Primary Endpoint Analysis

(b) (4) primary efficacy endpoint of spot tachogram-level PPV for AF will be estimated as follows:

$PPV_{Tachogram(AF)}$ = (# of spot tachograms classified as irregular according to the spot tachogram algorithm and where the paired ECG strip is classified as AF) / (# of spot tachograms classified as irregular according to the spot tachogram algorithm)

A one-sided 97.5% lower confidence bound will be computed using an unadjusted normal distribution approximation to the binomial. If the lower bound for the spot tachogram-level PPV exceeds (b) the null hypothesis, H_0, will be rejected.

(b) (4)

(b) (4) [redacted]

9.4. Secondary Endpoint Analysis

The alert-level (PPV) for AF will be estimated as follows (b) (4) [redacted]

$PPV_{Alert(AF)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF) / (# of alert notifications classified as AF according to the alert notification algorithm)

A two-sided exact 95% confidence interval will be computed.

(b) (4) [redacted]

9.5. Additional Analyses

For each of the additional endpoint analyses presented below two-sided 95% confidence intervals will be reported using an unadjusted normal distribution approximation to the binomial. A two-sided exact 95% confidence interval will be reported for the alert-level PPV for AF and other arrhythmias.

5.4.1. Spot Tachogram PPV for AF and Other Arrhythmias

The spot tachogram PPV for AF and other arrhythmias will be estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) [redacted]

$PPV_{Tachogram(AF\ and\ OA)}$ = (# of spot tachograms classified as irregular according to the spot tachogram algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of spot tachograms classified as irregular according to the spot tachogram algorithm)

5.4.2. Alert-Level PPV for AF and Other Arrhythmias

The alert-level (PPV) for AF and Other Arrhythmias will be estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) Each subject will contribute only one alert notification in this analysis.

$PPV_{Alert(AF\ and\ OA)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of alert notifications classified as AF according to the alert notification algorithm).

5.4.3. Spot Tachogram Sensitivity and Specificity

(b) (4) the spot tachogram sensitivity (for AF) and specificity (for Sinus Rhythm) will be calculated and reported along with the corresponding two-sided 95% confidence intervals.

(b) (4)

9.6. Safety Analyses

The number of serious adverse device effects (ADEs) and the number and percentage of subjects in this sub-study reporting each type of adverse event will be presented by adverse event coding categories. Multiple occurrences of the same event reported by the same subject will be counted only once.

10. Statistical Software

All analyses will be performed with SAS, v9.4 or higher and R (b) (4) in a Microsoft Windows environment.

11. Appendix (b) (4)

(b) (4)

DEN180042 / A002

Biologics CONSULTING | PHARMACEUTICALS, DEVICES & BIOLOGICS ADVISORS

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

September 6, 2018

Re: DEN180042
(b) (4) App

Dear Linda Ricci:

I am submitting this letter to request the following two adminstrative chnages for DEN180042.

1. (b) (4)
2. Change the name of the device to "Irregular Rhythm Notification feature"

The full contact information for the Submitter/Applicant is:

Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Please note that there is no change to the Primary Correspondent. It remains as:

Donna-Bea Tillman, Ph.D.
Senior Consultant
Biologics Consulting
1555 King St, Suite 300
Alexandria, VA 22314
410-531-6542
dtillman@biologicsconsulting.com

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of Apple Inc. or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must

comply with all provisions of 21 C.F.R. § 20.61(e), including by providing Apple Inc. with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions about this request, do not hesitate to reach out to me or other members of the team.

Sincerely,

(b) (6) [redacted]

Donna Bea Tillman, Ph.D
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

September 6, 2018

Re: DEN180042
(b) (4) App

Dear Linda Ricci:

I am submitting this letter to request the following two adminstrative chnages for DEN180042.

1. (b) (4)
2. Change the name of the device to “Irregular Rhythm Notification feature”

The full contact information for the Submitter/Applicant is:

Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Please note that there is no change to the Primary Correspondent. It remains as:

Donna-Bea Tillman, Ph.D.
Senior Consultant
Biologics Consulting
1555 King St, Suite 300
Alexandria, VA 22314
410-531-6542
dtillman@biologicsconsulting.com

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of Apple Inc. or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must

comply with all provisions of 21 C.F.R. § 20.61(e), including by providing Apple Inc. with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions about this request, do not hesitate to reach out to me or other members of the team.

Sincerely,

(b) (6)

Donna Bea Tillman, Ph.D
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

DEN180042

Biologics CONSULTING | PHARMACEUTICALS, DEVICES & BIOLOGICS ADVISORS

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

August 8, 2018

Re: de novo Submission
Submitter: (b) (4)
Device Name: (b) (4) App
Payment Identification Number: MD6103470

Dear Erdit Gremi:

I am submitting this de novo for the (b) (4) App, in accordance with the (b) (4) plan previously agreed to with FDA. The de novo contains all appendices as listed in the Table of Contents with the following exceptions:

- Appendix A2 – The User fee cover sheet was not previously included in the list of appendices (b) (4). It has been included as Appendix A2 of this de novo submission.
- Appendix E – As discussed with FDA, the clinical study report (Appendix E) will be provided as a supplement to this de novo for delivery to FDA on August 13.

Per FDA's request, we are providing in this de novo redlined versions of documents that were previously submitted during the review of (b) (4) where appropriate. Responses to FDA feedback during the review are (b) (4) are provided as Appendix P.

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

The ecopy contains the following three volumes:
VOL_001 Cover Letter and Main Body
VOL_002 Appendices
VOL_003 References

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of (b) (4) or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must comply with all provisions of 21 C.F.R. § 20.61(e), including by providing

Biologics Consulting Group, Inc.
1555 King Street, Suite 300 • Alexandria, Virginia 22314
Phone: 703.739.5695 • Toll Free: 800.485.0106 • Fax: 703.548.7457
BiologicsConsulting.com

(b) (4) with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions or concerns, do not hesitate to reach out to me or other members of the team. We really appreciate the opportunity to work with you to explore novel approaches for digital health product premarket reviews.

Sincerely,

(b) (6)

Donna Bea Tillman, Ph.D.
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

U.S. Food and Drug Administration
Center for Devices and Radiological Health
Document Control Center – WO66-G609
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

August 8, 2018

Re: de novo Submission
Submitter: (b) (4)
Device Name: (b) (4) App
Payment Identification Number: (b) (4)

Dear Erdit Gremi:

I am submitting this de novo for the (b) (4) App, in accordance with the (b) (4) plan previously agreed to with FDA. The de novo contains all appendices as listed in the Table of Contents with the following exceptions:

- Appendix A2 – The User fee cover sheet was not previously included in the list of appendices (b) (4) It has been included as Appendix A2 of this de novo submission.
- Appendix E – As discussed with FDA, the clinical study report (Appendix E) will be provided as a supplement to this de novo for delivery to FDA on August 13.

Per FDA's request, we are providing in this de novo redlined versions of documents that were previously submitted during the review of (b) (4) where appropriate. Responses to FDA feedback during the review are (b) (4) are provided as Appendix P.

The eCopy provided with this submission is an exact duplicate of the paper copy except that: (1) only the final signed cover letter was provided in paper form and (2) the eCopy includes all content.

The ecopy contains the following three volumes:
VOL_001 Cover Letter and Main Body
VOL_002 Appendices
VOL_003 References

This submission contains trade secret and confidential information. This information is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and may not be disclosed without the prior written authorization of (b) (4) or its affiliates. Such disclosure is prohibited by the U.S. Criminal Code, 18 U.S.C. § 1905, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j), and FDA regulations, 21 C.F.R. § 20.61(c). If FDA receives a request for this information and determines that disclosure may be appropriate, the Agency must comply with all provisions of 21 C.F.R. § 20.61(e), including by providing

Biologics Consulting Group, Inc.
1555 King Street, Suite 300 • Alexandria, Virginia 22314
Phone: 703.739.5695 • Toll [illegible]
BiologicsConsulting.com

(b) (4) with timely advance notice and a meaningful opportunity to object before making the disclosure, and a copy of any specific records the agency proposes to disclose.

If you have any questions or concerns, do not hesitate to reach out to me or other members of the team. We really appreciate the opportunity to work with you to explore novel approaches for digital health product premarket reviews.

Sincerely,

(b) (6)

Donna Bea Tillman, Ph.D.
Senior Consultant, Biologics Consulting Group
(410) 531-6542
dtillman@biologicsconsulting.com

(b) (4)

(b) (4) Mobile Medical App

De Novo Classification Request

August 7, 2018

Submitter	(b) (4)
Primary Submission Correspondent	Donna-Bea Tillman, Ph.D. Senior Consultant Biologics Consulting 1555 King St, Suite 300 Alexandria, VA 22314 410-531-6542 dtillman@biologicsconsulting.com
Secondary Submission Correspondent	Calley Herzog Senior Consultant Biologics Consulting 1555 King St, Suite 300 Alexandria, VA 22314 720-883-3633 cherzog@biologicsconsulting.com

TABLE OF CONTENTS

List of Appendices

1. CDRH PREMARKET REVIEW SUBMISSION COVER SHEET

See Appendix A for the completed cover sheet, FDA Form 3514.

2. COVER LETTER

The final, signed cover letter is provided as a separate PDF document on the eCopy of this submission.

3. INDICATIONS FOR USE

(b)(4) - Draft

[redacted]

See Appendix B for the Indications for Use Statement, FDA Form 3881.

4. ADMINISTRATIVE INFORMATION

This *De Novo* submission is prepared in accordance with FDA Draft Guidance Document "*De Novo* Classification Process (Evaluation of Automatic Class III Designation)" issued on October 30, 2017.

4.1. Device Name

Device Common Name: Irregular Rhythm Analysis Software

Device Trade / Proprietary Name: (b) (4) Mobile Medical App

4.2. Submitter and Contact Information

Submitter Name: (b) (4)

Primary Submission Correspondent:

Donna-Bea Tillman, Ph.D.
Senior Consultant
Biologics Consulting
1555 King St, Suite 300
Alexandria, VA 22314
410-531-6542
dtillman@biologicsconsulting.com

Secondary Submission Correspondent:

Calley Herzog
Senior Consultant
Biologics Consulting
1555 King St, Suite 300
Alexandria, VA 22314
720-883-3633
cherzog@biologicsconsulting.com

4.3. Statements Certifications and Declarations of Conformity

N/A

5. REGULATORY HISTORY

5.1. Prior Submissions

(b) (4)

6. DEVICE OVERVIEW

6.1. Introduction

As is well recognized, Atrial Fibrillation (AF) is one of the most common serious cardiac arrhythmias, and when left untreated, is a leading cause of morbidity and mortality from stroke, heart failure, and myocardial infarction.[1,2]

Early detection and treatment of patients with AF minimizes risk of sequelae of thromboembolism including >60% reduced risk of stroke.[3,4] However, many affected with AF are unaware they have this arrhythmia due to a number of factors including lack of symptoms, or experience only mild symptoms that they do not attribute to the disease.[5] As a result, asymptomatic patients are three times as likely to have sustained an ischemic stroke prior to diagnosis than those with symptoms.[6,7] These findings raise concerns and have prompted several variations of screening programs to identify patients with asymptomatic AF and prevent an embolic event.[8,9] While systematic and opportunistic screening programs have demonstrated increased rates of detection when compared to detection during routine clinical practice, such screening programs are not yet widely implemented.[10] Additionally, AF may be paroxysmal (PAF, or intermittent AF) and therefore missed by recording a single in-clinic ECG, especially for those with intermittent symptoms. Holter devices are commonly used for ambulatory 24-hour ECG monitoring in at-risk patients, but have limited sensitivity for the detection of new AF.[11]

The (b) (4) App provides users the opportunity to take advantage of a background, opportunistic measuring tool intended to identify and notify the user of episodes of irregular heart rhythms. This approach to obtaining health information is consistent with the shifting paradigm for how medical care is delivered in the US. Traditionally, the US population has surrendered control of their healthcare information to their Healthcare Provider (HCP). This traditional model is often referred to as the "acute-care paradigm,"[12] and over the past two decades a significant shift has occurred. HCPs are no longer the sole holders of medical knowledge as consumers become the primary authorities of their own health information.[13] This is desirable for a number of reasons and is supported by a widely-referenced Institute of Medicine report that showed improving healthcare quality often depends on patients' involvement.[14] This shift in paradigm allows for patients to partner more closely with their healthcare care providers and further engage in their healthcare decisions.

This paradigm shift in healthcare is also supported by multiple federal legislative efforts. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and Centers for Medicare and Medicaid Services Incentive Program of 2014 for the Meaningful Use of Electronic Health Records both encourage the use of electronic health records through

financial incentives for US hospitals. Related efforts by the U.S. Department of Health and Human Services (HHS) and other federal agencies, such as the Blue Button e-Health Program and endorsement of the Fast Healthcare Interoperability Resources (FHIR) standards, are currently underway to bolster individuals' access to their health records. As a result, approximately half of the US hospitals and 40 percent of physicians provide portals that allow patients to access their medical records and manage their health information.[15] Patients who have access to their medical records have reported a broader knowledge of their own health issues, which allows them to communicate more effectively with their physicians. These patients are also more likely to initiate efforts to improve their health, which has been shown to lead to a decreased utilization of healthcare services.[16,17,18]

6.2. Clinical Background

Atrial fibrillation (AF), the most common sustained serious cardiac arrhythmia with an estimated lifetime risk of one in four,[19,20] accounts for 15% of the 700,000 strokes per year in the United States.[21] In one study,[22] up to one-third of all strokes were attributable to AF. The prevalence of AF in the United States is estimated to be between 3 and 6 million,[23] and this number is expected to rise sharply to over 12 million by 2030[24] due to an aging population and a rising age-adjusted incidence of AF. Oral anticoagulation (OAC) has been shown to substantially reduce the risk of AF associated stroke.[25] However, 18% of AF-related strokes occur in patients with asymptomatic or subclinical AF that is newly-detected at the time of stroke.[26] Asymptomatic and subclinical AF have been associated with similar morbidity and mortality rates as symptomatic AF,[27] and with similar rates of silent embolic events.[28] Moreover, untreated AF substantially increases the risk of the development of heart failure and other cardiac complications. Therefore, earlier detection of asymptomatic or subclinical AF could reduce the total public-health burden of ischemic stroke, heart failure, and other AF-related sequelae with upstream therapies.

With an aging population in which AF prevalence is forecasted to increase substantially,[29] effective AF screening strategies may have important public health implications. These tools are not intended to replace the physician, but rather to augment the patient-provider relationship.

Guidelines for AF Screening

Contemporary international guidelines on primary prevention of AF-related stroke, and general guidelines on AF management, recommend opportunistic pulse detection (pulse palpation by trained health care personnel during routine health care contact) in patients ≥ 65 years of age.[30] In Europe, the newest 2016 guideline recommendations from the European Society of Cardiologists (ESC) allow for the replacement of pulse palpation with an ECG rhythm strip as an appropriate method of AF screening.[31]

While mass screening has yet to be recommended in younger populations, there is mounting evidence that demonstrates early management of the disease may prevent progression to permanent disease as well as other conditions such as structural heart disease.[32] Also has been increasing thought to be related to structural heart diseasFurthermore, increasing evidence exists around lifestyle modification and its ability to prevent disease and the progression of disease.[33] Devices such as the one described in this submission are needed to clarify the effectiveness of screening both in young and at-risk populations to better understand the natural history of the disease, prevention of disease, downstream health outcomes, cost-effectiveness, and impact on healthcare utilization.

Prevalence of Undiagnosed AF

Prior work indicates a high rate of undiagnosed AF in the general population. In a back calculating modeling study based on incidence of AF shortly following ischemic stroke in Medicare and commercial claims beneficiaries, there are an estimated 500,000 persons with undiagnosed AF in the United States, with an estimated incremental cost burden of $3.2 billion.[34]

However, given the paroxysmal and asymptomatic nature of AF, brief intermittent screening strategies are highly insensitive and likely to only capture patients with high AF burdens. This issue is highlighted by a study that demonstrated use of a handheld intermittent ECG monitor for 30 days improved detection of AF episodes compared to 24-48 hours of continuous ECG monitoring.[35] Similarly, the investigation of prolonged ambulatory ECG screening (30 days) for AF after stroke, as compared to conventional 24-hour Holter monitors, detected 5-fold more AF (16.1% vs. 3.2%).[36] With improvements in AF detection algorithms, long-term implantable cardiac monitors (ICM) are being increasingly used to screen for occult AF with recent studies in people equipped with ICMs demonstrating an average time to detection of AF of 123 days.[37] However, the benefits of long-term screening with this modality come with the downsides of an invasive procedure and high cost and are therefore not widely recommended. Given the limited wear-time of current ECG monitoring technologies, it is likely that a small but significant portion of the population remain undiagnosed despite normal screening mechanisms. This population would likely benefit from an easily available, opportunistic, non-invasive screening mechanism like the (b) (4) App.

Wearable Health Technologies

Recently, there has been substantial uptake, both from consumers and patients, of wearable health technology such as wrist-worn devices incorporating multiple sensors. Such technologies can generate large amounts of real-time data on patient activity and heart rate variability, often through photoplethysmography (PPG)-based measurements of capillary blood volume. As

technologies advance and adoption increases, wearable health technologies will be able to deliver increasingly more complex information on patient health. To date, these data sources have largely been focused on monitoring activity and have shown some early benefits in the treatment of obesity and diabetes.[38,39] However, efficient utilization of wearable cardiac data to effect improvement in traditional patient outcomes has been limited. For decades, cardiac implanted electronic devices (e.g., pacemakers and implantable cardioverter defibrillators) have collected and transmitted real time patient data, ranging from measures of patient activity to life-threatening arrhythmia notifications. These systems have been shown to improve clinical outcomes (e.g., time to clinical decision and mortality) and serve as proof of concept for wearable health technology based patient monitoring, but come with risk.

6.3. Device Description

The (b) (4) App comprises a pair of mobile medical apps, one on Apple Watch and the other on the iPhone. The (b) (4) Watch App analyzes pulse rate data collected by the Apple Watch PPG sensor to identify episodes of irregular heart rhythms consistent with AF and provides a notification to the user. It is a background screening tool and there is no way for a user to initiate analysis of pulse rate data. The (b) (4) iPhone App is part of the Health App, which allows users to store, manage, and share health and fitness data, and comes pre-installed on every iPhone. Users must opt-in and go through on-boarding prior to use of the (b) (4) App.

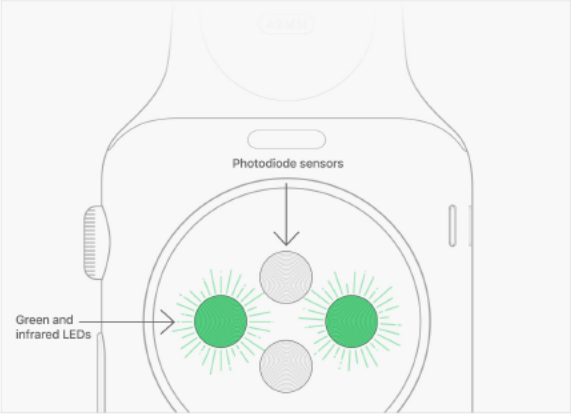
The (b) (4) App is not intended to diagnose atrial fibrillation, and is not intended to be used to guide clinical treatment or care.

Platform/PPG

The (b) (4) App leverages heart rate data collected from the commercially available PPG sensor on Series 1 and later Apple Watch platforms. The Apple Watch uses green LED lights paired with light−sensitive photodiodes to detect relative changes in the amount of blood flowing through a user's wrist at any given moment. When the heart beats it sends a pressure wave down the vasculature, causing a momentary increase in blood volume when it passes by the sensor. By monitoring these changes in blood flow the Apple Watch can measure the heart rate. Further, under stationary conditions the sensor can detect individual pulses when they reach the periphery and thereby measure the beat-to-beat intervals.

A schematic of the sensors on the Apple Watch is provided in Figure 6-1 below.

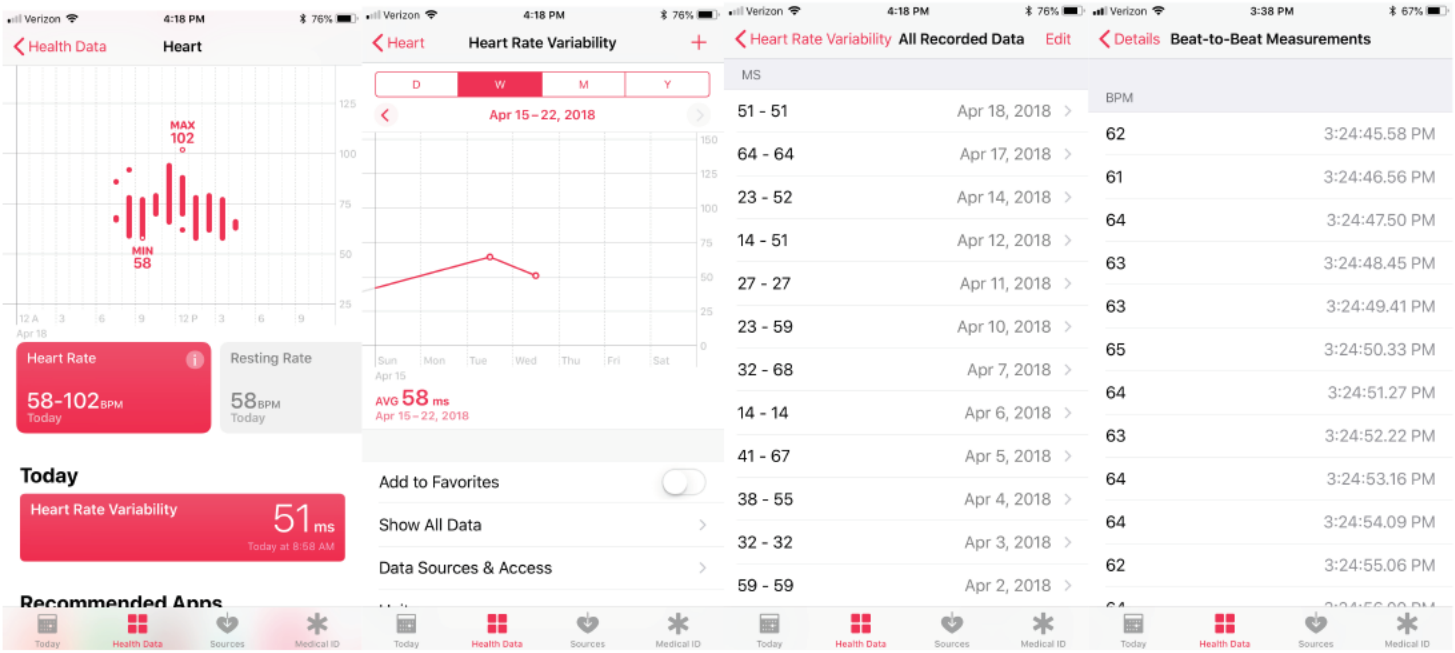
Figure 6-1 Schematic of Apple Watch Sensors



Currently, Apple Watch attempts to collect and analyze a one-minute beat-to-beat sequence (called a "tachogram") in the background (i.e., with no user action required) approximately every 4 hours, depending on user activity. A minimum of (b) (4) pulses is required for a measurement to be considered successful and stored in HealthKit; measurements are stored as beat-to-beat time intervals. Measurements that do not meet the specification are discarded and never surfaced to the user in any form. Measurements that meet the specification are surfaced to the user as a Heart Rate Variability (HRV) value accessible within the Health App on the iPhone; Apple Watch calculates HRV using the standard deviation of the beat-to-beat intervals within the tachogram (also known as SDNN).

The current user interface for HRV on iPhone is shown below in Figure 6-2. The fourth screen below shows the beat-to-beat measurements during a one minute tachogram.

Figure 6-2 Current User Interface for HRV



(b) (4) Watch App

The (b) (4) Watch App refers to the tachogram classification algorithm, confirmation cycle algorithm, and the AF notification generation. Tachogram analysis is initiated when the (b) (4) Watch App retrieves a new tachogram from Watch HealthKit. Tachograms are classified as either irregular or not AF. If a sufficient number of tachograms are retrieved and classified to meet the notification threshold (5 of 6 sequential tachograms classified as irregular within a 48-hour period), a notification indicating that the heart rhythm has shown signs of AF will be displayed to the user. This process is further described in Principles of Operation: (b) (4) Algorithm section below. Individual tachogram classification results for sequences that do not meet the notification threshold are not accessible to the user.

If an irregular heart rhythm consistent with AF is identified, the (b) (4) Watch App will transfer the AF notification to the (b) (4) iPhone App through HealthKit sync.

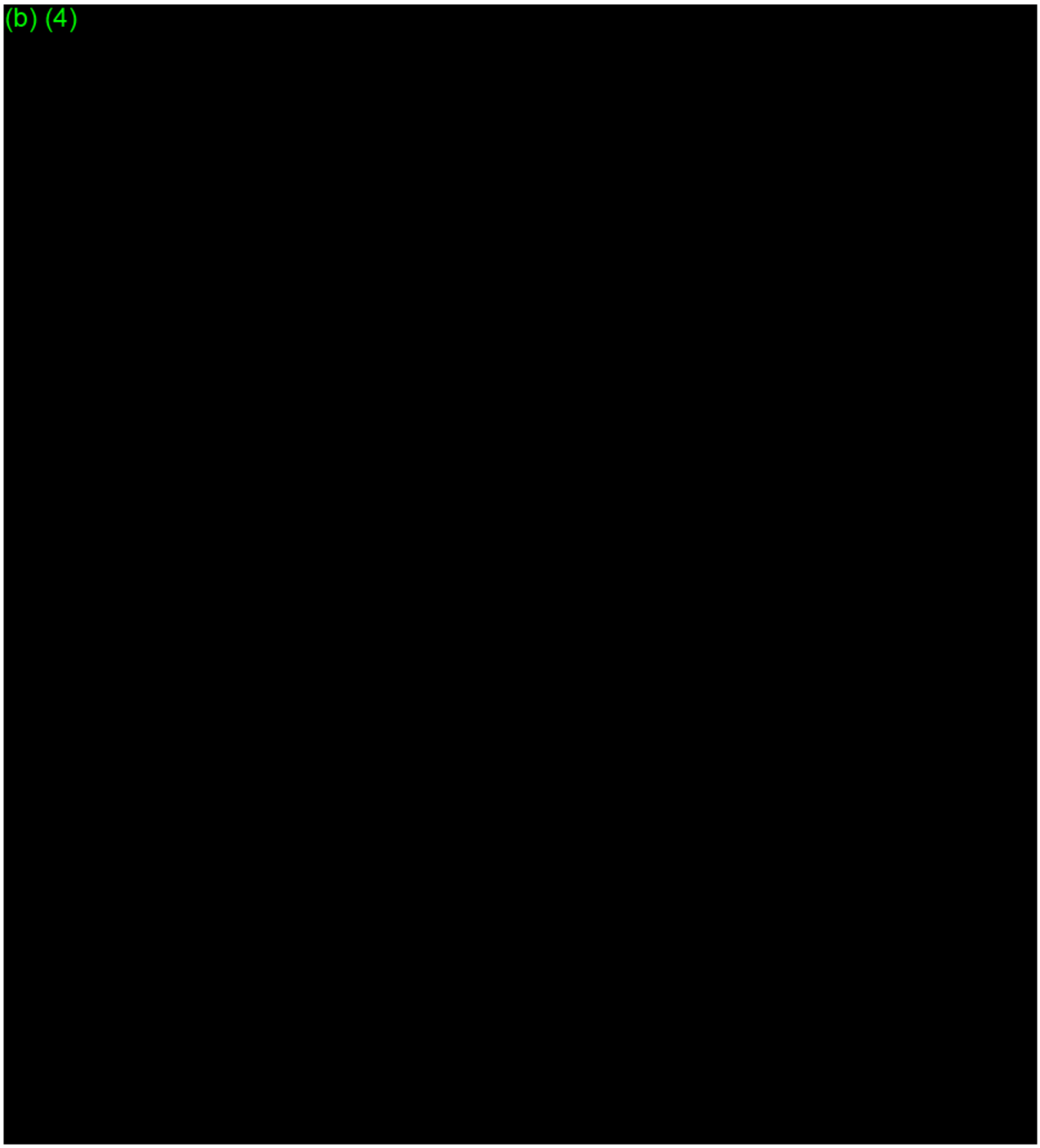
In addition to indicating the finding of signs of AF, the notification will encourage the user to seek medical care if they have not previously been diagnosed with AF.

(b) (4) iPhone App

Apple considers the (b) (4) iPhone App to be the (b) (4) User Interface (UI) Framework as well as the information included in the Atrial Fibrillation Notification portion of the Health App. The (b) (4) UI Framework contains the on-boarding and educational materials that a user must review prior to enabling AF notifications. The (b) (4) iPhone App is designed to work in combination with the (b) (4) Watch App and will display a history of all prior atrial fibrillation notifications. The user is also able to view a list of times when each of the irregular tachograms contributing to the notification was generated.

An example of a display of atrial fibrillation notification history is provided in Figure 6-3.

Figure 6-3 Atrial Fibrillation Notification History



6.4. Principles of Operation: (b) (4) Algorithm

(b) (4)

There are two major modules of the (b) (4) Watch App that analyze pulse rate data and identify irregular heart rhythms consistent with AF — one that classifies a tachogram as irregular or not AF (referred to as the "tachogram classification algorithm"), and the other for the confirmation cycle, which determines if a notification will be surfaced to the user (the "confirmation cycle algorithm"). At baseline, the Watch platform will attempt to capture a tachogram every 4 hours to support the commercially available HRV feature. Once the (b) (4) App is installed, the Watch platform will attempt to capture a tachogram every 2 hours and notify the (b) (4) App when a new tachogram is captured and available for analysis. When the (b) (4) Watch App retrieves a tachogram, it assesses the degree and pattern of variability to classify it as irregular or not AF. If a tachogram is classified as irregular, the "confirmation cycle" begins, during which the (b) (4) Watch App requests additional tachograms from the platform more frequently (as frequently as possible subject to a minimum spacing of 15 minutes). If five out of six sequential tachograms (including the initial one) are classified as irregular within a 48-hour period, a notification of this finding is surfaced to the user. If two tachograms are classified as not AF before this threshold is reached, the (b) (4) Watch App returns to baseline (attempting to retrieve tachograms every 2 hours), no results are surfaced, and the confirmation cycle is reset (that is, any irregular tachograms within this sequence do not count in future confirmation cycles).

(b) (4)

(b) (4)

6.5. Proposed Conditions of Use

The (b) (4) App is intended for over-the-counter use to opportunistically identify irregular heart rhythms consistent with AF. It is not intended for use in a clinical setting or to guide clinical treatment or care.

6.6. Device Components

The (b) (4) App comprises two apps: the (b) (4) Watch App and the (b) (4) iPhone App. The Watch App analyzes the pulse rate data and identifies irregular heart rhythms consistent with AF. The (b) (4) iPhone App provides the user with on-boarding and access to educational information. In addition, the (b) (4) iPhone App receives AF notifications from the (b) (4) Watch App through HealthKit Sync and displays a history of AF notifications for the user to reference.

6.7. System Accessories

General purpose platforms - Apple iPhone (5s or later) with iOS version 12.0 or later and Apple Watch (Series 1 or later) with watchOS version 5.0 or later.

6.8. Materials

(b) (4) is a software-only device; therefore, this section is not applicable.

6.9. Sterilization & Shelf Life

(b) (4) is a software-only device; therefore, this section is not applicable.

6.10. Packaging

(b) (4) is a software-only device; therefore, this section is not applicable.

6.11. Alternative Practices and Procedures

FDA has not cleared any devices using PPG technology to identify irregular heart rhythms consistent with AF. There are cleared blood pressure cuffs that identify irregular heart rhythms using the pulse at the periphery (see, e.g., K151330, Microlife Wrist Watch Blood Pressure Monitor; K163045, Omron Wrist Blood Pressure Monitor). Those devices, however, use oscillometric, rather than PPG technology. There are FDA-cleared ECG devices that can be used in the home to detect atrial fibrillation (see, e.g., K142743, AliveCor Kardia Mobile; K171816, AliveCor Kardia Band System) but those devices require an initial clinician consult prior to use, and use ECG, rather than PPG, technology. Additionally, each of the aforementioned devices is for on-demand use. Apple is not aware of any devices that operate using a background, opportunistic means of measuring pulse rate to identify irregular heart rhythms consistent with AF.

7. PROPOSED DEVICE CLASSIFICATION

7.1. Predicate Review

7.1.1. Classification Searches

Apple searched the FDA Product Classification and 510(k) databases to determine if FDA has previously cleared any over-the-counter devices that use PPG technology to identify irregular heart rhythms. The following table lists the product codes and classification regulations that were considered.

Product Code	Classification Regulation
DXH (Telephone electrocardiograph transmitter and receiver)	870.2920 Telephone electrocardiograph transmitter and receiver
MHX (Physiological Patient Monitor with Arrhythmia Detection or Alarms)	870.1025 Arrhythmia detector and alarm
DSI (Arrhythmia detector and alarm)	870.1025 Arrhythmia detector and alarm
DQA (Oximeter)	870.2700 Oximeter
DXN (Noninvasive blood pressure measurement system)	870.1130 System, Measurement, Blood-Pressure, Non-Invasive
JOM (Hydraulic, pneumatic, or photoelectric plethysmographs)	870.2780 Plethysmograph, Photoelectric, Pneumatic or Hydraulic

7.1.2. Similar Devices

Examples of devices that were considered as potential predicate devices are provided in the table below, along with the device's intended use and how the cleared device compares to the proposed device.

Device	Indication for Use	Comparison
K110374, Medicore Max Plus System	Provides noninvasive measurement of pulse waveform and heart rate by photoelectric plethysmography. Indicated for use in hospitals, health care clinics, and physicians' offices.	While using PPG technology, the intended use is different. The (b) (4) App is intended for identifying irregular heart rhythms, while this device is cleared for measuring waveform and heart rate. This device is also cleared for Rx, not OTC, use.
K142743, AliveCor Kardia Mobile	Intended to record, store and transfer single-channel electrocardiogram (ECG) rhythms. It also displays ECG rhythms and detects the presence of atrial fibrillation and normal sinus rhythm (when prescribed or used under the care of a physician).	This device uses ECG, rather than PPG technology. It is also cleared for a combination Rx/OTC use, rather than solely OTC.

K151269, LifeWatch ECG Mini System Continuous ECG Monitor and Arrhythmia Detector	Intended for use by patients who experience transient symptoms that may suggest cardiac arrhythmia. The device continuously monitors patient ECG, automatically generates an alarm triggered by an arrhythmia detection algorithm, or generates an alarm manually triggered by the patient, and transmits the recorded data to a monitoring center, which provides the ECG data to the medical practitioner for evaluation.	This device uses ECG rather than PPG technology, and is intended for Rx rather than OTC use.
K151330, Microlife Wrist Watch Blood Pressure Monitor	Intended to measure the blood pressure and pulse rate by using a non-invasive oscillometric technique in which an inflatable cuff is wrapped around the wrist. The device detects the appearance of irregular heartbeat during measurement and gives a warning signal with the reading once the irregular heartbeat is detected.	This device does not use PPG technology, and is primarily intended for use as a blood pressure monitor.

K163045, Omron Wrist Blood Pressure Monitor	The device is a digital monitor intended for use in measuring blood pressure and pulse rate. The device detects the appearance of irregular heartbeats during measurement and gives a warning signal with readings.	This device does not use PPG technology, and is primarily intended for use as a blood pressure monitor.
K171816, AliveCor Kardia Band System	Intended to record, store and transfer single-channel electrocardiogram (ECG) rhythms. It also displays ECG rhythms and detects the presence of atrial fibrillation and normal sinus rhythm (when prescribed or used under the care of a physician). The Kardia Band System is intended for use by healthcare professionals, adult patients with known or suspected heart conditions and health conscious individuals.	This device uses ECG, rather than PPG technology. It is also cleared for a combination Rx/OTC use, rather than solely OTC.

7.1.3. Why (b) (4) App is Different

As seen in the table above, there does not appear to be a suitable predicate device for the (b) (4) App. The devices that use PPG technology are not intended for use to identify irregular heart rhythms, and the devices that do detect irregular heart rhythms do not use PPG technology. Therefore, the (b) (4) App is different from currently marketed devices, and can properly be regulated through the *de novo* pathway.

7.2. Classification Recommendation

Apple proposes that the (b) (4) App be classified as a Class II device, Irregular Rhythm Analysis Software, subject to general and special controls. Pursuant to section 515(a)(1)(C) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) (21 U.S.C. 360c(a)(1)(C)), Class III devices are those that are purported or represented to be for a use in supporting or sustaining human life or for a use which is of substantial importance in preventing impairment of human health, or that presents a potential unreasonable risk of illness or injury. The (b) (4) App does not meet this definition of a Class III device. It is not purported or represented to be for a use in supporting or sustaining human life, it is not for a use which is of substantial importance in preventing impairment of human health, and it does not present a potential unreasonable risk of illness or injury. Rather, it is intended for use as a background, opportunistic means of identifying irregular heart rhythms consistent with AF. It is not intended as a diagnostic device, and it provides a means by which people may be directed to their clinicians earlier than would be done through current standard of care. Users will also be able to better understand their heart rates and heart rhythms in relation to their overall health, thus providing users more control over and insight into their personal health information. Given this intended use of the device, it does not meet the definition for a Class III device. The potential risks of the (b) (4) App are also comparable to those of other OTC device types that FDA has classified as Class II, including non-invasive blood pressure devices and pregnancy test kits, and the (b) (4) App presents significantly less risk than other OTC Class II devices, such as blood glucose meters.

Apple has proposed below the special controls that it believes are adequate, in conjunction with the general controls set forth in the FD&C Act, to demonstrate reasonable assurance of safety and effectiveness of the device type Irregular Rhythm Analysis Software.

7.3. Proposed Special Controls

Apple proposes that, in combination with general controls, the Irregular Rhythm Analysis Software should be subject to the following special controls:

(b) (4)

8. SOFTWARE DOCUMENTATION

8.1. Statement of Level of Concern

The software level of concern for the (b) (4) App is **Moderate**.

This determination was reached by a careful review of the FDA guidance document "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices - Guidance for Industry and FDA Staff" (5/11/2005). The following list of questions and answers gives a summary of that decision making process:

Questions for Major Level of Concern

1. Does the Software Device qualify as Blood Establishment Computer Software?

   No

2. Is the Software Device intended to be used in combination with a drug or biologic?

   No

3. Is the Software Device an accessory to a medical device that has a Major Level of Concern?

   No

4. Prior to mitigation of hazards, could a failure of the Software Device result in death or serious injury, either to a patient or to a user of the device? Examples of this include the following:

   a. Does the Software Device control a life supporting or life sustaining function?

      No

   b. Does the Software Device control the delivery of potentially harmful energy that could result in death or serious injury, such as radiation treatment systems, defibrillators, and ablation generators?

      No

   c. Does the Software Device control the delivery of treatment or therapy such that an error or malfunction could result in death or serious injury?

No

d. Does the Software Device provide diagnostic information that directly drives a decision regarding treatment or therapy, such that if misapplied it could result in serious injury or death?

No

e. Does the Software Device provide vital signs monitoring and alarms for potentially life threatening situations in which medical intervention is necessary?

No

Questions for Moderate Level of Concern

1. Is the Software Device an accessory to a medical device that has a Moderate Level of Concern?

   No

2. Prior to mitigation of hazards, could a failure of the Software Device result in Minor Injury, either to a patient or to a user of the device?

   No

3. Could a malfunction of, or a latent design flaw in, the Software Device lead to an erroneous diagnosis or a delay in delivery of appropriate medical care that would likely lead to Minor Injury?

   Yes. A malfunction or latent design flaw in the (b) (4) App could lead to a delay in delivery of appropriate medical care.

Based on the answers to question #3 above, the software level of concern for the (b) (4) App is **Moderate**.

8.2. Software Description

As this is a standalone software device, the device description and algorithm description provided above (Sections 6.3 and 6.4) describe the device features and intended operational environment. The following information is provided according to the software guidance:

- Programming language: C, C++, Objective C
- Hardware platform: Apple Watch Series 1 or later, iPhone 5s or later
- Operating system (if applicable): watchOS 5.0, iOS 12.0
- Use of Off-the-Shelf software: Provided in Appendix G

8.3. Device Hazard Analysis

The device hazard analysis was provided in Module 2. The revised Hazard Analysis is provided in Appendix H (clean) Appendix H1 (redlined).

(b) (4)

A usability risk analysis was also performed to address the foreseeable use errors. A copy of the usability risk analysis is provided in the HFE report (Appendix D).

8.4. Software Requirements Specification (SRS)

The Software Requirements Specification was provided in Module 2. Updates were made in response to FDA feedback on Module 2 and for clarification. See redlined and clean versions in Appendix I1 and Appendix I, respectively.

8.5. Architecture Design Chart

The (b) (4) Software Architecture document provided in Module 1 was updated and is included in Appendix C (clean) and Appendix C1 (redlined).

8.6. Software Design Specification (SDS)

The Software Design Specification was provided in Module 2. Updates were made to address FDA's request for more detailed information. See Appendix J.

8.7. Traceability Analysis

The Traceability Analysis is provided in Appendix N.

8.8. Software Development Environment Description

Apple has established procedures for software design and development, configuration management, and maintenance plans.

(b) (4)

(b) (4)

8.9. Verification and Validation Documentation

Software verification will be completed to verify that all predefined requirements have been fulfilled and that the software satisfies the intended use and user needs. Verification Test Results are included in Appendix O. (b) (4) Validation is completed through Human Factors testing and Clinical Validation testing.

This section describes end-to-end design verification testing for the (b) (4) App to show that the requirements outlined in the SRS in Appendix I and Appendix I1, clean and redlined respectively, are met.

There are two subsets of design verification testing - (b) (4)

(b) (4)

(b) (4)

8.10. Revision Level History

(b) (4)

8.11. Unresolved Anomalies (Bugs or Defects)

(b) (4)

8.12. Cybersecurity

This information was provided in Module 2. Minor updates have been made to account for updates to the Instructions for Use language. See Appendix K and Appendix K1 for clean and redlined versions, respectively. The iOS Security Guide is included in Appendix K2.

8.13. Basic Documentation for Off-the-Shelf Software

Basic Information for Off the Shelf software was provided in Module 2. Minor updates were made to account for the hazard line items associated with OTS software. See Appendix G (clean) and G1 (redlined).

9. SUPPORTING PROTOCOLS AND/OR DATA

9.1. Platform Requirements

9.1.1. Safety

All Apple Watch products are evaluated to demonstrate compliance with applicable thermal safety, battery safety, and RF and EMC for emission and immunity guidelines. A summary of the applicable guidelines and associated testing is provided below.

9.1.1.1. Thermal Safety Testing

To prevent a thermal hazardous situation when a user makes contact with the external surface of the platform, Apple requires that the Apple Watch series 4 (final finished product for product release) is tested and shown to be in compliance with applicable thermal safety requirements of IEC 60950-1, *"Information Technology Equipment – Safety Part 1: General Requirements."* and IEC 62368-1, *"Audio/video, information and communication technology equipment - Part 1: Safety requirements"* before the product is released. The requirements of IEC 62368-1 are similar to the requirements from IEC 60601-1 "Medical electrical equipment –Part 1: General requirements for basic safety and essential performance". The thermal safety (external surface) requirements specified for the Apple Watch are summarized in Table 9-1.

Table 9-1 Thermal Safety Requirements (External Surface)

Usage Mode	Material Type	Maximum Temperature During Normal Use (°C)		
		*IEC 60950-1 Requirement	**IEC 62368-1 Requirement	*IEC 60601-1 Requirement
Discharge mode (devices worn on the body in direct contact with skin)	Metal	55	43	43
	Glass	65	43	43
	Plastic	75	43	43
Discharge mode (surfaces likely to be touched while in use)	Metal	55	48	48
	Glass	65	48	48
	Plastic	75	48	48
Charging mode (Inductive charger and restore connector)	Metal	60	51	51
	Glass	70	56	56
	Plastic	85	60	60

*Surface temperature limits for all operating ambient temperatures; Apple defines the maximum operating ambient temperature

**Surface temperature limits while tested in a 25°C ambient

9.1.1.2. RF and EMC Testing for Emission and Immunity

Apple also requires the Apple Watch to be tested and shown to comply with US FCC Part 15 Rules for radio frequency devices and EN 301 489-17 V 3.2.0 "Electromagnetic Compatibility Standard for Radio Equipment – Part 17: Specific conditions for Broadband Data Transmission Systems." To date, all released Apple Watch products have met the requirements of not emitting electromagnetic disturbance that could affect other radio frequency services and essential performance of other equipment. The Apple Watch has been shown to maintain adequate immunity to electromagnetic disturbance during operation.

FCC ID is posted on the regulatory page under settings in each product. Declarations of Conformity for EN 301 489-17 V 3.2.0 is posted on Apple website at https://www.apple.com/euro/compliance/.

9.1.1.3. Battery

To address the concerns of fire hazards and to prevent the product from being the source of combustion, the batteries from both the released Apple Watch and iPhone products are tested and certified to the standards in Table 9-3.

Table 9-3 Battery Certifications

Battery Type	Certification
Cell	• IEC 62133 Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications • UL1642 Standard for Lithium Batteries • CTIA Certificate - IEEE 1725 Requirements for Rechargeable Batteries for Cellular Telephones
Pack (Cell and battery management unit)	• IEC 60950-1 Medical electrical equipment –Part 1: General requirements for basic safety and essential performance • IEC 62133 Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications • UL 2054 Standard for Household and Commercial Batteries • CTIA Certificate - IEEE 1725 Requirements for Rechargeable Batteries for Cellular Telephones

9.2. Platform Performance Testing

The (b) (4) App leverages heart rate data collected from the commercially available PPG sensor on Series 1 and later Apple Watch platforms. The Apple Watch uses green LED lights paired with light−sensitive photodiodes to detect relative changes in the amount of blood flowing through a user's wrist at any given moment.

Apple Watch attempts to collect and analyze a tachogram in the background. A minimum of (b) (4) pulses is required for a measurement to be considered successful and stored in HealthKit; measurements are stored as beat-to-beat time intervals. Measurements that do not meet the specification are discarded and never surfaced to the user in any form. Measurements that meet the specification are surfaced to the user as a Heart Rate Variability (HRV) value accessible within the Health App on the iPhone; Apple Watch calculates HRV using the standard deviation of the beat-to-beat intervals within the tachogram (also known as SDNN).

(b) (4)

9.3. (b) (4) App Performance Testing

Apple plans to submit the following testing to support the performance of the (b) (4) App. These are described in detail in the sections below.

- Algorithm development and engineering testing (Section 9.3.1, below)
- Software design verification testing (Section 8.9, above)
    - Results are included in Appendix O.
- Software validation
    - Human factors testing (Study report included in Appendix D)
    - Clinical validation testing (Updated protocol included in Appendix E; (b) (4)

9.3.1. Algorithm Development

Apple conducts rigorous data collection and engineering testing in order to develop and tune its algorithms.

During initial development of the (b) (4) algorithm (described in the Principles of Operation: (b) (4) Algorithm section above), Apple conducted a variety of engineering studies to collect data used for core algorithm development.

Subsequent targeted studies were used to validate initial findings, better understand a wider variety of users and use cases, ensure algorithm robustness to these conditions, and build a more diverse dataset for algorithm refinement and tuning. Most importantly, these studies were used to expand understanding of the algorithm performance under various identified factors which can potentially affect PPG signals. Algorithm changes were made as a result of these studies to target specific failure modes.

9.3.1.1. (b) (4) Algorithm Development

(b) (4)

Table 9-4 Overview of Algorithm Development Studies

(b) (4)

9.3.2. Human Factors Testing

Our HFE/UE Report, per the Guidance, "Applying Human Factors and Usability Engineering to Medical Devices," is included in Appendix D. A high level discussion of the results and residual risks are provided below.

9.3.2.1. Tested Product v. Final Product

(b) (4)

(b) (4)

9.3.2.2. HFE/UE Summary

The study included a total of 37 participants from the two user groups for the (b) (4) App:

- Individuals who have concern regarding arrhythmias and have an active interest in monitoring potential arrhythmias ("Active Interest", n=16), and
- Individuals who do not have concern regarding arrhythmias and do not have an active interest in monitoring potential arrhythmias but who might use the app out of casual or passing interest ("Passive Interest", n=21).

Both groups included participants with and without past experiences with iPhones and Apple Watches.

A summary of the participant demographics are included below.

Table 9-5 Summary of participant demographics

Gender	Passive	Active
Male	7	2
Female	14	14

Age	Passive	Active
22-64	13	11
65+	8	5

Education	Passive	Active
High School or Less	5	1
Some College	4	9
College Degree	7	6
Post-graduate	5	0

Smart Accessory Experience	Passive	Active
Apple Watch	8	4
Garmin	0	1
FitBit	1	3
None	12	8
Smartphone Experience	**Passive**	**Active**
iPhone	15	15
Android	3	0
None	3	0

All participants set up the app, which was meant to simulate the actual on-boarding process. The participants then experienced a decay period of approximately 1 hour, and then a testing session that lasted approximately 30 minutes. Sessions took place in a simulated home environment, which is representative of an expected environment of use in real life. Both observational data and subjective evaluations were collected.

Overall, usability testing demonstrated that the (b) (4) App is safe and effective for the intended users, uses, and use environments. In particular:

- 36/37 participants successfully responded indicating that a lack of a notification from the App would not affect their medical decisions.

- 35/35 participants successfully received a notification and indicated they would not reduce care if experiencing acute symptoms.

(b) (4)

(b) (4)

9.4. Animal

Not applicable.

9.5. Clinical

The Apple Heart Study (AHS) is a prospective, observational study currently being conducted by Stanford Medicine, American Well, BioTelemetry, and Apple (the Study Sponsor). Enrollment began on November 30, 2017 and ended on August 1, 2018.

The AHS was initiated to understand the true prevalence of undiagnosed atrial fibrillation (AF) in a large population in order to better understand the utility of this diagnosis in the asymptomatic population, and to notify those who did not know they have AF of its presence and potential risk of stroke.

The purpose of the AHS Sub-Study is to conduct an analysis on a pre-specified subset of data collected in AHS to support a regulatory submission before the AHS ends. Individual tachograms (beat-to-beat intervals) taken from a user's Watch at the same time they are wearing the gold standard ECG patch (ePatch provided by BioTelemetry) as well as notifications that occur during patch wear will be used to determine if the tachogram classification algorithm and confirmation cycle algorithm have acceptable positive predictive value (PPV).

Because in real-world use only individuals who receive a notification will receive follow-up diagnostic care (unless a clinician otherwise believes such care is appropriate), the population of interest for performance measurement is exactly those users who receive a notification. Hence the AHS protocol calls for gold standard ECG patch data on a post-alert population, and the endpoints of the study focus on data collected during simultaneous Apple Watch and ePatch wear. This population, while enriched, also reflects the real-world downstream impact of the (b) (4) App.

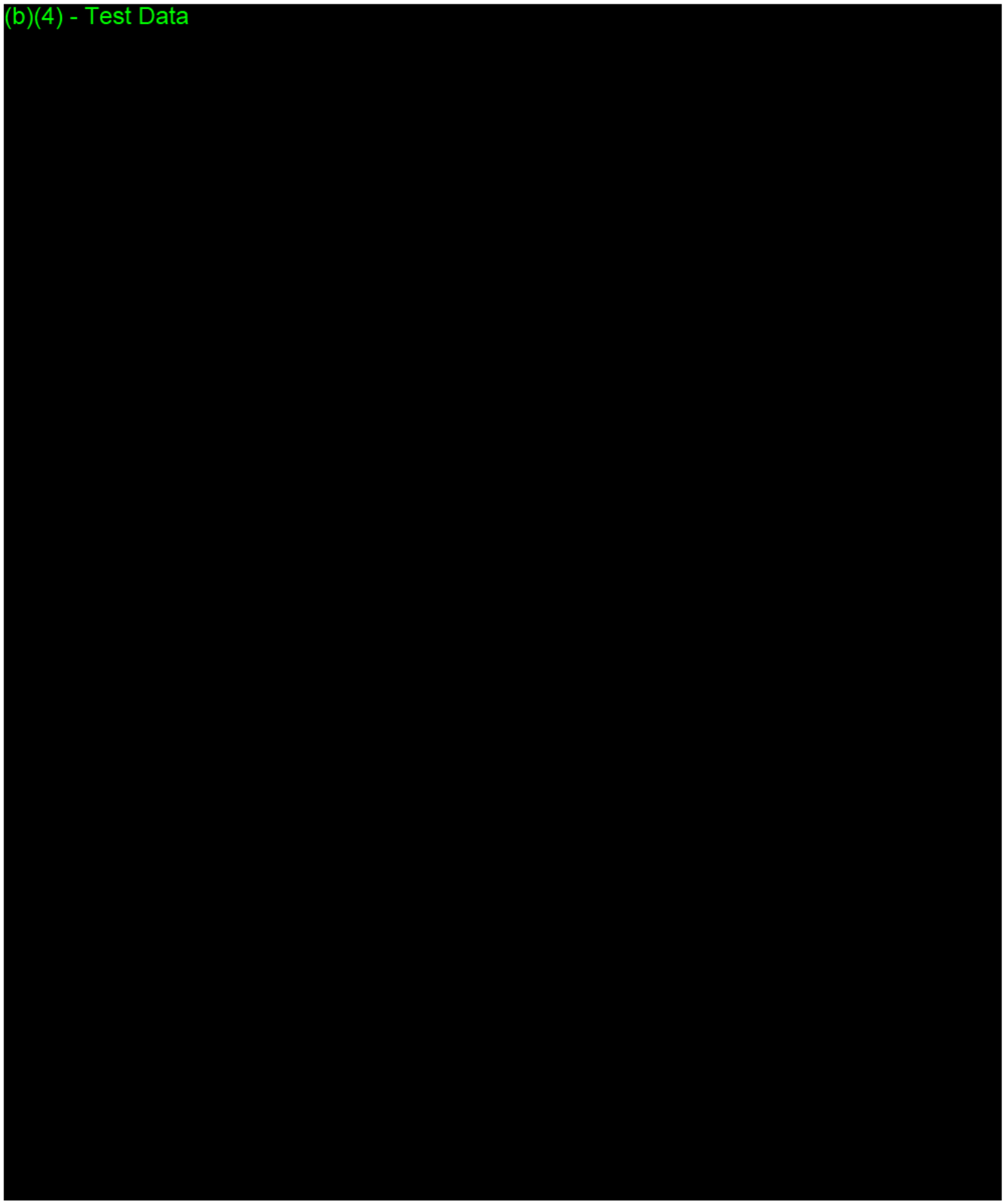
The objective of the AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory ECG patch monitoring in identifying irregular rhythms consistent with AF.

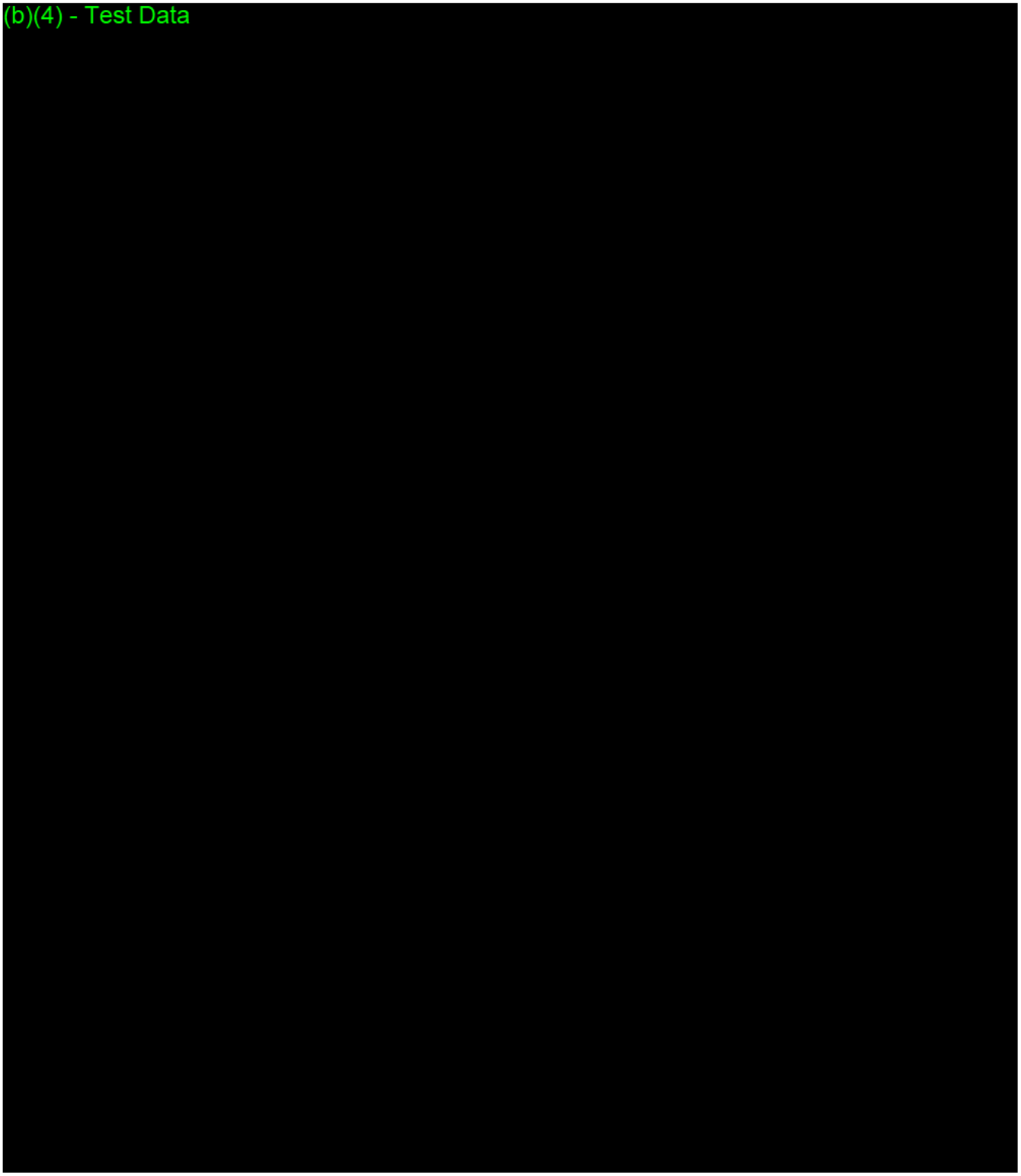
The study endpoints are as follows:

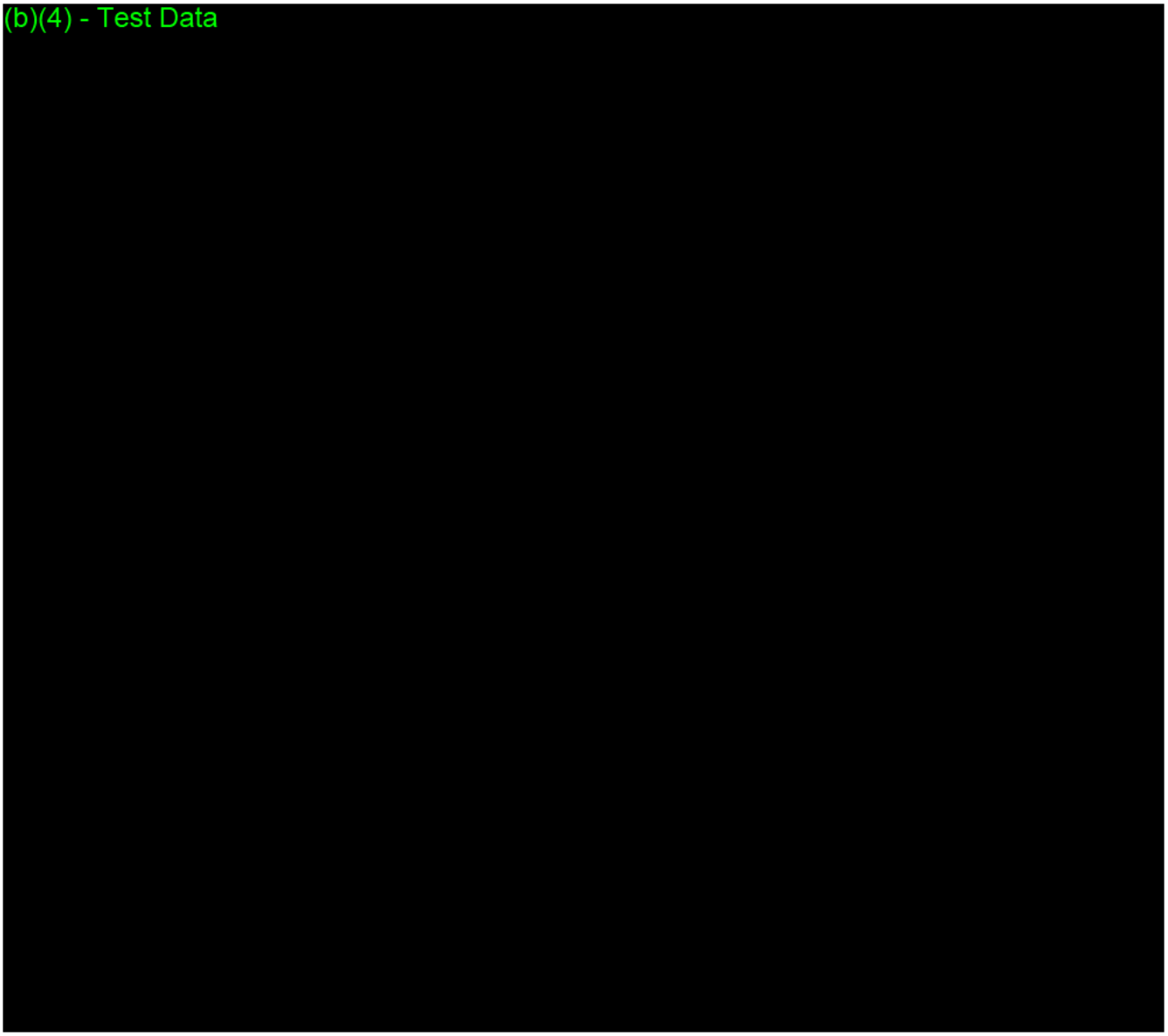
- Primary Efficacy Endpoint: Identification of irregular rhythm consistent with AF as suggested by positive predictive value (PPV) of the spot tachogram [Spot Tachogram PPV] where the ECG patch readings (paired to the timestamp associated with the spot tachograms) are used for the determination of AF.
- Secondary Efficacy Endpoint: Identification of irregular rhythm consistent with AF as suggested by PPV of the alert [Alert-Level PPV] (based on multiple irregular tachograms) where the ECG patch readings are used for the determination of AF.
- Primary Safety Endpoint: Incidence of serious adverse device effects (ADEs).

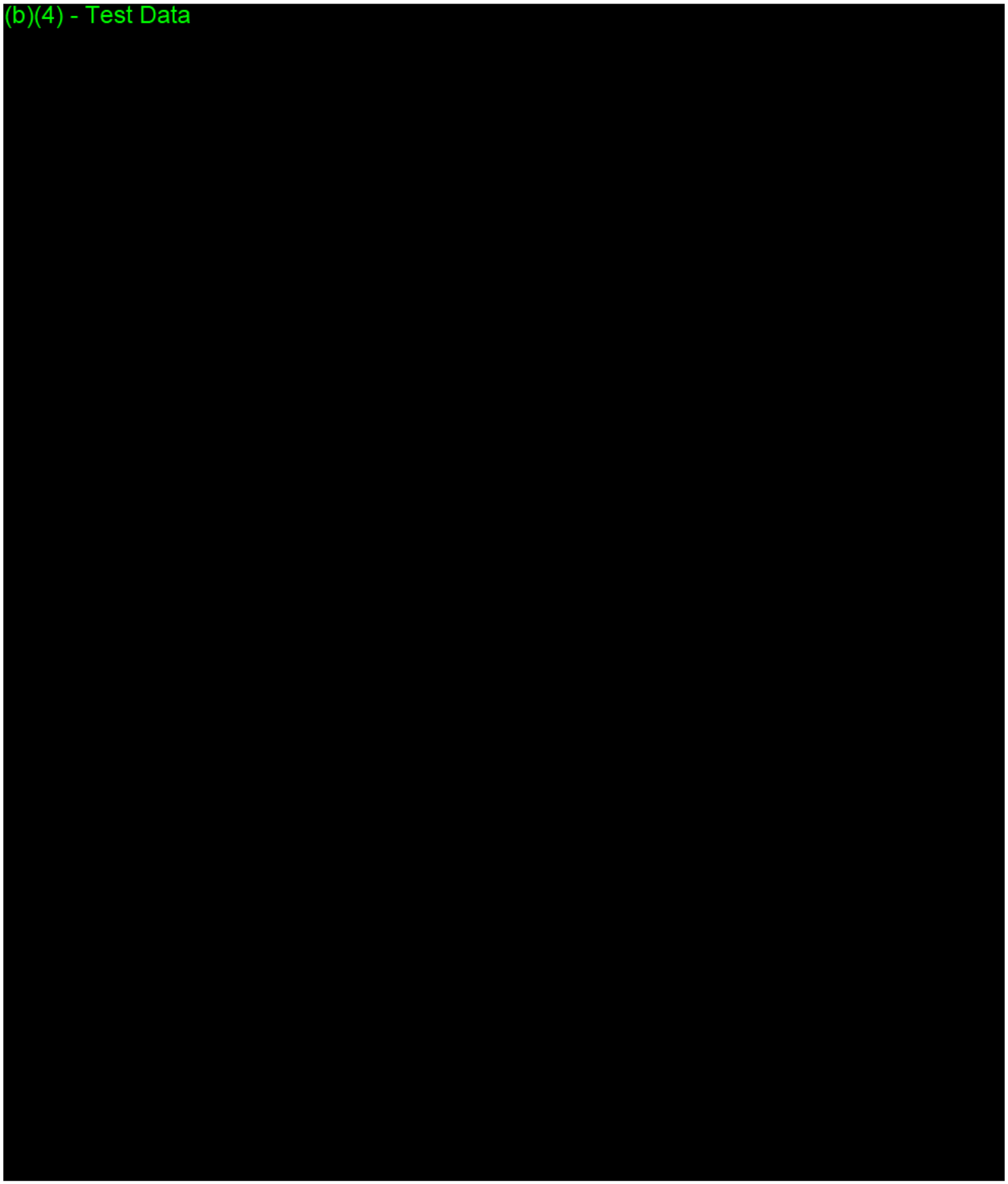
The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b) There were no hypotheses specified for the secondary endpoint or the safety endpoint.

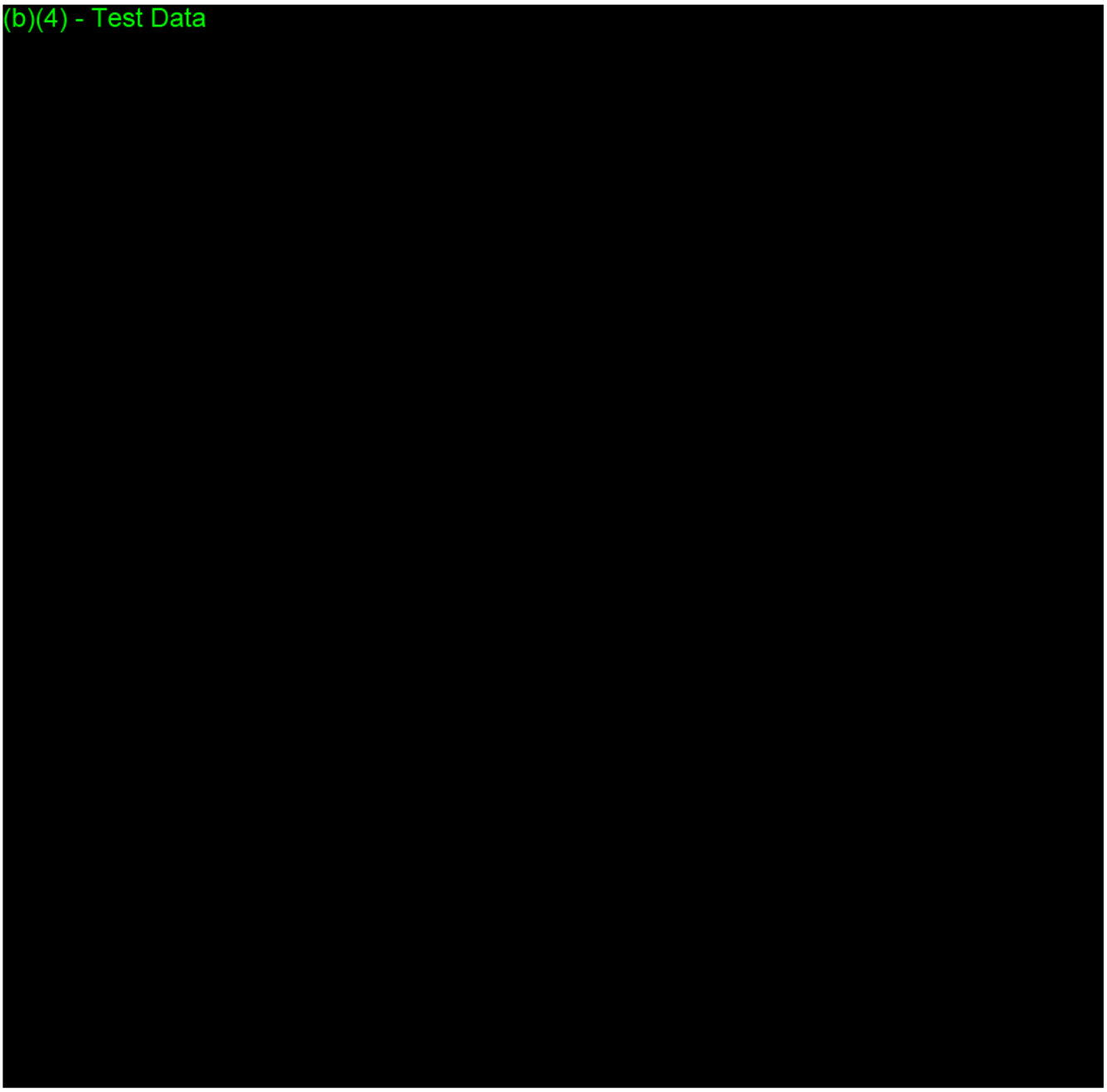
(b) (4)

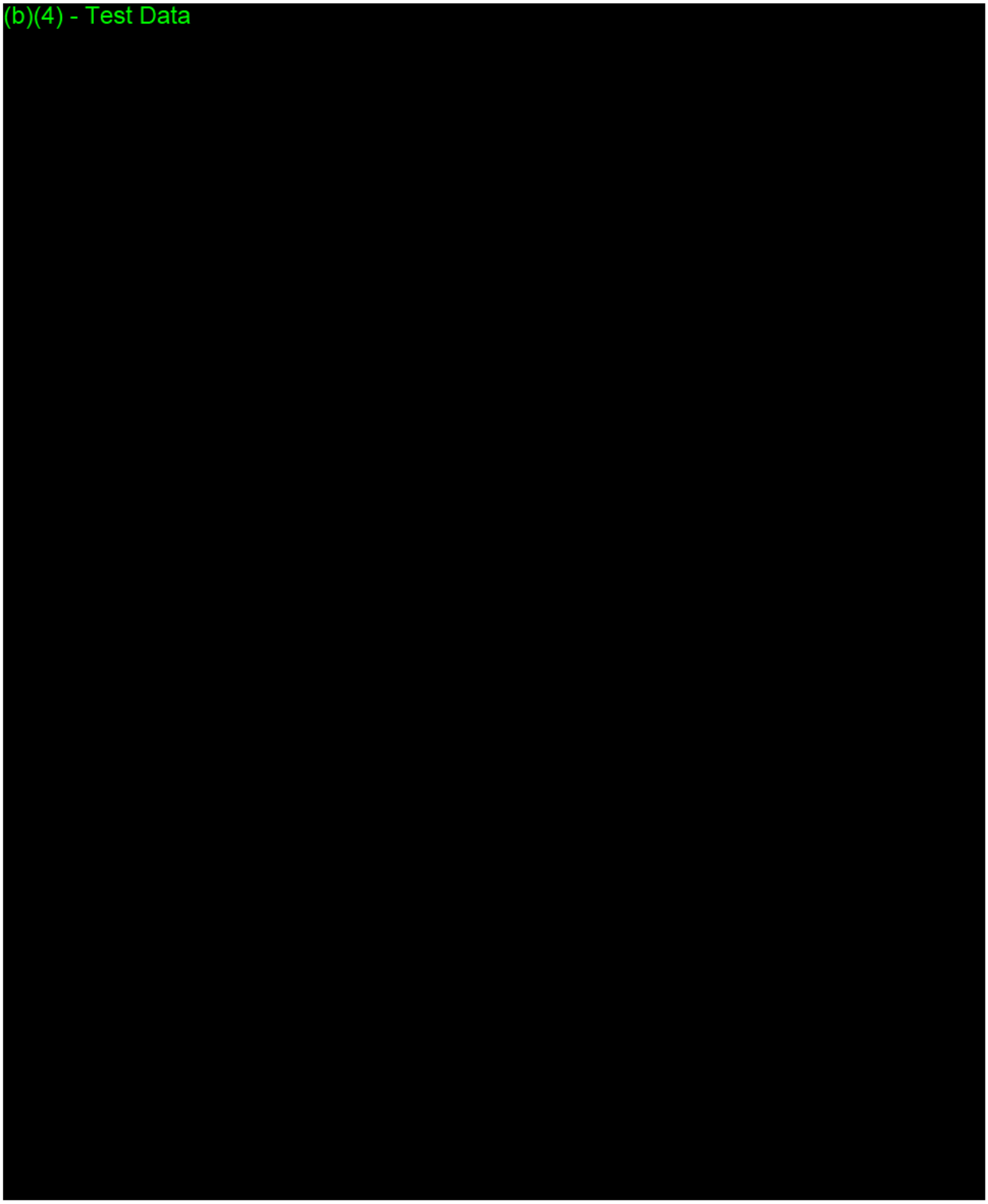




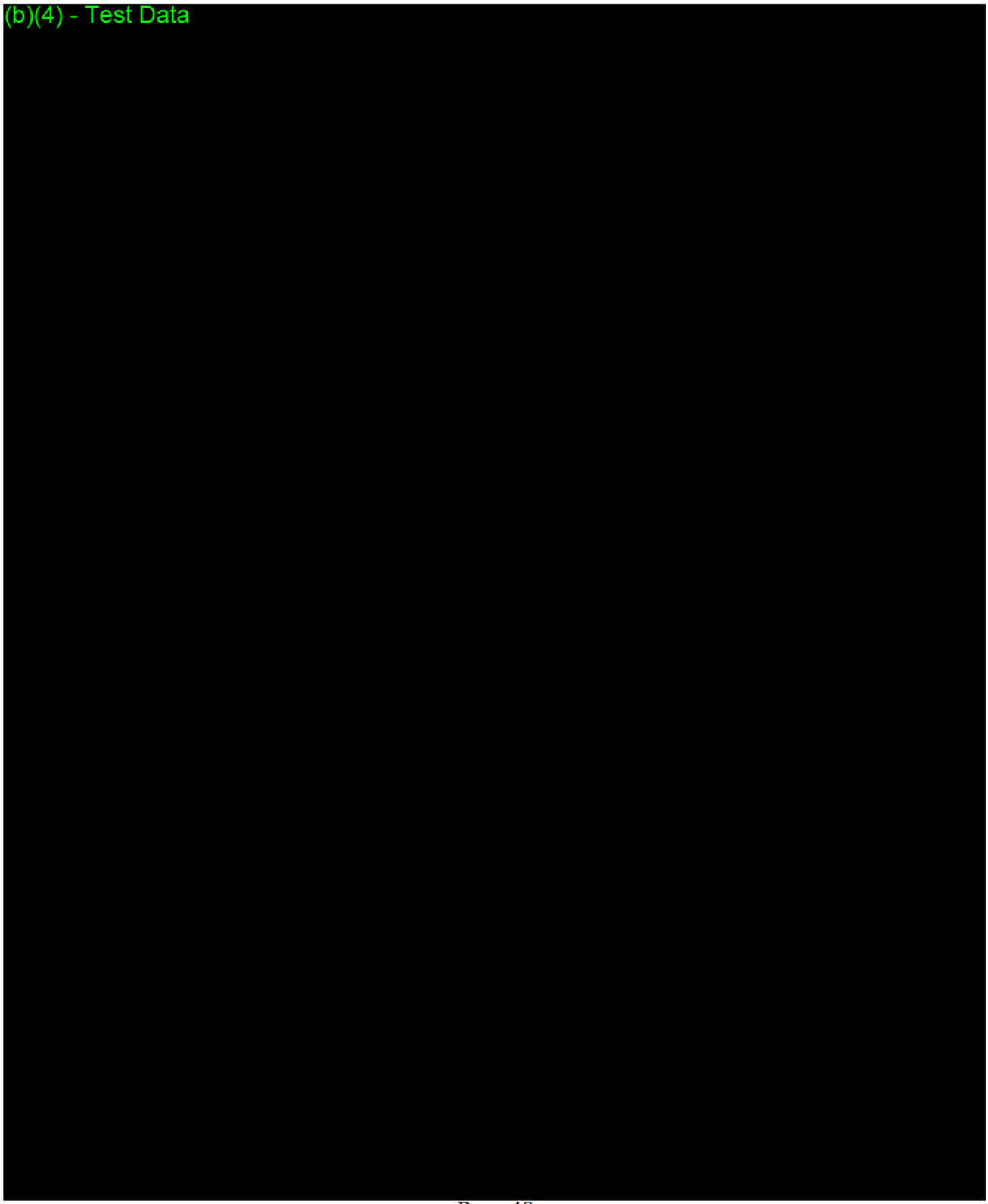








(b)(4) - Test Data



10. SUMMARY OF BENEFITS

Per FDA's guidance document, "Factors to Consider When Making Benefit Risk Determinations in Medical Device Premarket Approval and De Novo Classifications" (Benefit-Risk Guidance), FDA considers the following factors when assessing the probable benefits of the device: the type of benefit, magnitude of benefit, probability of the patient experiencing one or more benefits, and the duration of the effects. Each of these is considered below.

Type of Benefit

One of the key benefits of the (b) (4) App is that it provides something that does not exist today-an opportunity for background, opportunistic minimally invasive and passive checks for irregular heart rhythms consistent with AF. As the device can be worn for extended periods of time, it is likely that it will pick up episodes of AF that would otherwise have gone undetected through traditional methods. This ability to detect AF over longer periods of time is valuable as recent studies have shown that prolonged screening over 30 days as compared to traditional 24-hour Holter monitors detected 5-fold more AF,[45] and in studies with implantable loop recorders, the average time to detection of AF was 123 days.[46]

For asymptomatic individuals, an AF notification may serve as the "symptom" that encourages them to seek further medical care. Providing individuals with a passively detected signal could allow them to seek further medical evaluation that could eventually lead to an earlier diagnosis of AF or other serious clinically significant arrhythmias in otherwise asymptomatic individuals.

Early diagnosis of AF is significant for multiple reasons. Mounting evidence demonstrates early management of the disease may prevent progression to permanent disease.[47] Furthermore, increasing evidence exists around lifestyle modification and its ability to prevent disease and the progression of disease.[48] For young individuals <55 yo, AF has been associated with higher mortality than matched controls without AF,[49] and the presence of AF in these patients should prompt clinical evaluation for the presence of other disease including structural heart disease, thyroid abnormalities, and substance abuse.[50] For both younger and older individuals, early detection and treatment of AF can minimize the risk of sequelae of thromboembolism including >60% reduced risk of stroke.[51,52]

Products such as the (b) (4) App can improve the detection of AF in a manner that carries far less risk than invasive methods such as implantable cardiac monitors or loop recorders.

Magnitude of Benefit

The magnitude of the benefit can potentially be significant at both an individual user level as well as on a societal level.

As discussed in section 6.1 and 6.2, stroke as a result of AF is common and can lead to devastating health consequences.[53] Further, up to 16% of individuals with cryptogenic stroke were found to have evidence of AF,[54] suggesting a significant undiagnosed burden. An individual who receives a notification and seeks additional care may get diagnosed with AF earlier than would be likely in the current standard of care model. This may result in the individual finding significant benefit from avoided morbidity and mortality due to stroke.

At a societal level, recent estimates suggest 10-15% of AF is currently undiagnosed (>700,000 individuals in the US), with many of these individuals estimated to be at relatively higher stroke risk.[55] Identifying these individuals earlier and entering them into clinical evaluation pathway that could lead to earlier diagnosis of AF could prevent thousands of stroke events and related co-morbidities, as well as the societal cost.

Probability of the patient experiencing one or more benefits

Data from the AHS are able to provide insight into the probability of the patient experiencing one or more benefits. Information about the number of currently enrolled participants and corresponding notifications and notification rates is provided in Table 10-1 below.

Table 10-1 AHS Enrollment and Notification Rate Data as of August 3, 2018

	Age Buckets					
	22-39	**40-54**	**55-64**	**65+**	**Unknown**	**Total**
Enrolled	230,593	138,800	44,637	26,040	201	440,271
Notifications	287	415	504	667	1	1,874
Notification Rate	0.12%	0.30%	1.13%	2.56%	0.50%	0.43%

The information above demonstrates that the notification rates are consistent with the known prevalence of AF in the general populations. Although the Notification Rates are lower in the younger populations, they are not zero. This suggests that use of the (b) (4) App could provide people not previously diagnosed with AF, including younger and asymptomatic

individuals, with an opportunity to learn about possible AF well before they would otherwise in the current standard of care model.

Duration of effects

Early detection and treatment of patients with AF minimizes risk of sequelae of thromboembolism including >60% reduced risk of stroke.[56,57] In the case of lower-risk individuals where treatment is not indicated by guidelines, the appropriate follow-up may be "watchful waiting" and management of lifestyle factors that influence risk over time. Therefore, if the (b) (4) App notifies an individual that he or she has an irregular heart rhythm consistent with AF, and that individual seeks medical care and receives an AF diagnosis earlier than would have occurred in current standard of care, the effect of that early detection may positively influence the remainder of the individual's life.

11. SUMMARY OF IDENTIFIED RISKS TO HEALTH

The (b) (4) App is a low-risk app that presents minimal risks to health of the user. The AHS has allowed Apple a unique opportunity to assess possible risks associated with the product in the general intended user population.

The risk assessment process included evaluation of product design risks, usability risks, and cybersecurity risks. OTS software was also considered as part of the risk assessment taking into account the FDA guidance of OTS Software Use in Medical Device.

An updated copy of the risk assessment is provided in Appendix H and Appendix H1, clean and redlined respectively. Usability risk is provided in the HFE/UE report in Appendix D.

(b) (4)

FDA's Benefit-Risk Guidance sets forth the criteria by which it assesses the extent of the probable risks or harms of the device. These criteria are discussed in turn below.

Severity, types, number and rates of harmful events associated with the use of the device

Preliminary adverse event data from the AHS indicate that, as of August 3, 2018, with over 440,000 enrolled subjects, there have been only ten adverse device effects. None of these ten was

determined to be a serious adverse device effect, and all were related to anxiety. These data demonstrate that the direct risks to health associated with use of the (b) (4) App are expected to be minimal.

(b) (4)

Probability of a harmful event

FDA's guidance document defines probability as "the proportion of the intended population that would be expected to experience a harmful event" and further notes that "FDA would factor whether an event occurs once or repeatedly into the measurement of probability."

Until a product is marketed, it is difficult to assess with certainty the probability of theoretical harmful events occurring. The AHS does provide some insight into events that may occur through use of the (b) (4) App. As of August 3, 2018, with an enrollment of over 440,000 people, there have been only ten non-serious device-related adverse events, all related to anxiety. (b) (4) it is possible that individuals may delay care in the absence of a notification when experiencing mild to moderate symptoms. To Apple's knowledge, no such event has occurred over the course of the AHS; it therefore may be more theoretical than probable. Even if it were to occur, as discussed, harm would only be likely to occur in a unique set of circumstances: an individual feels mild to moderate symptoms while experiencing a serious condition, and elects to delay care due to not receiving a notification. The likelihood of this occurrence is minimal, and, as noted, has not, to our knowledge, happened during the duration of the AHS.

Duration of harmful events

In most cases, possible harmful events will not be long-lasting. For example, a user who experiences anxiety upon receiving a notification should then follow up with a clinician for further information and assistance regarding disease management.

In certain cases, as discussed above, it is possible that someone who ignores the product's labeling could suffer longer-term effects. For example, in the case of a symptomatic person experiencing an acute condition who does not receive a notification and fails to contact emergency services, harm could result. As noted, the likelihood of such an occurrence is

expected to be minimal, as a very specific sequence of events would need to occur for harm to materialize.

Risk from false-positive or false-negative results for diagnostics

Given Apple's broad user base, mitigating against the likelihood of false positives was a primary consideration during algorithm development. Therefore, as described in Section 6.4 above, the algorithm has been designed to require successful completion of a "confirmation cycle" before notifying the user to the possible presence of an irregular heart rhythm, in order to mitigate false positives to the greatest extent possible. The benefit of this design is demonstrated through the AHS Sub-Study results. While the PPV of each individual tachogram was approximately 66%, the PPV at the alert-level was approximately 79%. This demonstrates that the confirmation cycle properly mitigates against the likelihood of false positive results.

In the event that an individual were to receive a false positive notification, it is possible that the individual may be subjected to unnecessary clinical consultation or ECG monitoring. An unnecessary clinical consultation may be inconvenient, but does not likely present risk to the individual. ECG monitoring is not an invasive procedure, and does not carry significant risk. The most likely harms associated with ECG monitoring include skin irritation, anxiety, and misdiagnosis resulting from use of a previously FDA-cleared device.

There is also the possibility that the (b) (4) App will fail to correctly identify irregular heart rhythms consistent with AF, and will therefore fail to notify the user of such irregularities. As discussed in Section 12, there are mitigations built in to reduce this risk. For example, product labeling indicates a user should contact a clinician any time the user believes he is experiencing acute symptoms, even if he does not receive a notification from the (b) (4) App. HFE testing demonstrated that users understood that if they were experiencing serious symptoms, they should seek emergency care, notwithstanding the absence of a notification.

Furthermore, because users are likely to wear Apple Watch more than 12 hours per day, the misidentification of any single tachogram as regular rather than irregular does not mean the user will never be notified of the presence of AF. For asymptomatic individuals who would not otherwise be screened for AF, a slight delay in learning of a possible heart rhythm irregularity is not likely to have any clinical impact, since they will still potentially learn of the irregularity sooner than if the device were not used at all.

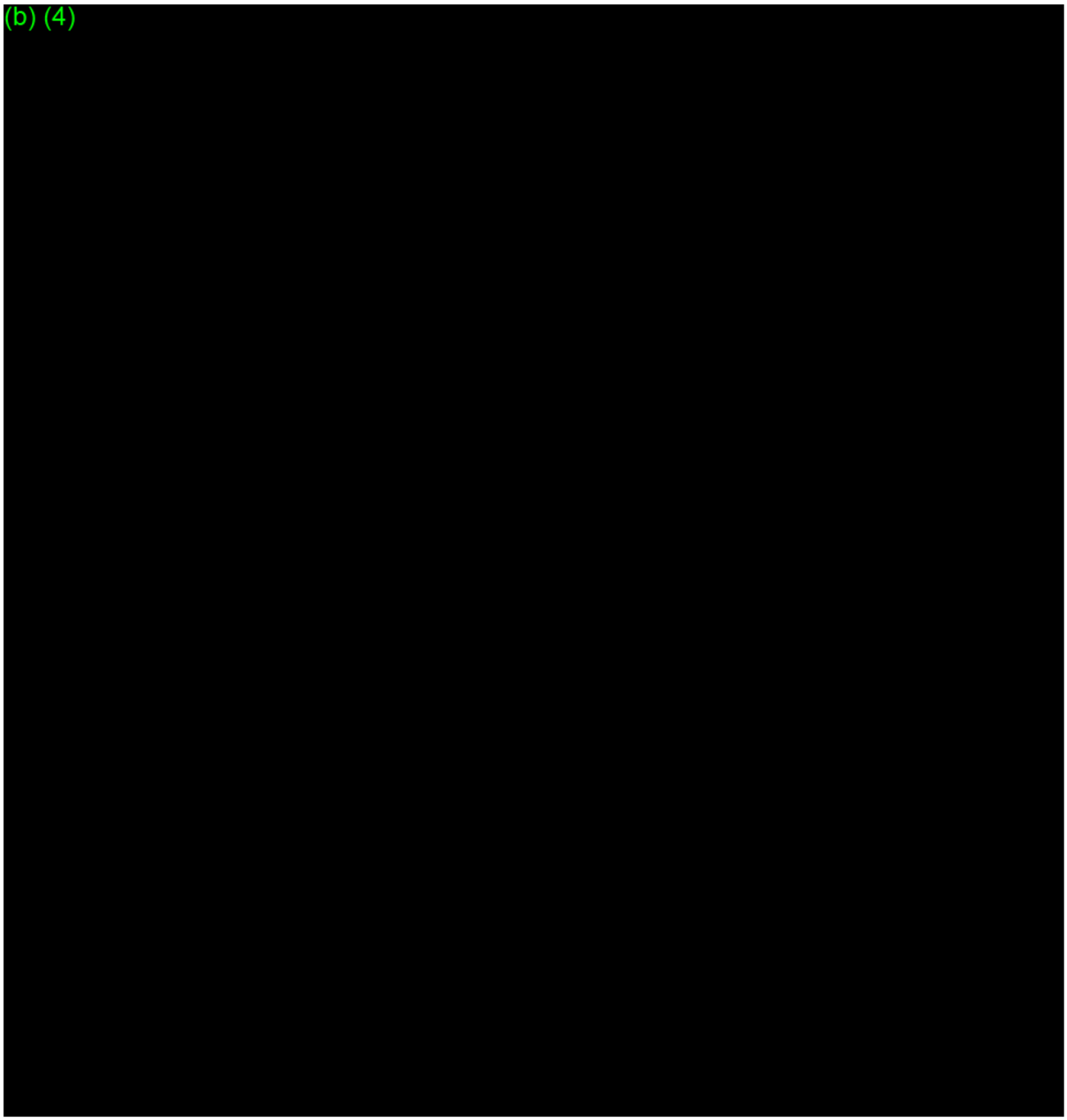
Given the non-invasive nature of the app, users will be likely to accept the possible risks associated with use of the device in order to reap the benefit of learning about possible irregularities much earlier than would otherwise be possible.

11.1. MAUDE Database Search (if applicable)

Given the novel nature of the (b) (4) App, and the lack of any similar products on the market, a MAUDE database search is not applicable.

12. RISK AND MITIGATION INFORMATION

(b) (4)



13. BENEFIT-RISK CONSIDERATIONS

As discussed above, FDA's guidance document, "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval and De Novo Classifications," outlines the factors FDA considers when making benefit-risk determinations. Importantly, FDA notes that when making benefit-risk determinations, it considers "probable" risks and benefits, not "theoretical" risks and benefits. The probable benefits and risks of the device have been discussed in detail in the sections above.

FDA also describes additional factors that it considers when assessing the probable benefits and risks of devices. Relevant additional factors are discussed below.

Uncertainty

FDA considers the degree of certainty of the benefits and risks of a device, while recognizing that it is not possible to be 100% certain of a device's reasonable assurance of safety and effectiveness. As described above, a key benefit of the (b) (4) App is that it would be the only marketed product that allows for background, opportunistic identification of irregular heart rhythms. Given the number of hours each day that people wear their Apple Watches, this background tool provides a unique opportunity to identify irregular heart rhythm in asymptotic individuals not previously diagnosed with AF.

The AHS was designed to take into account the broad user base of Apple Watch, and to demonstrate that device performance is suitable across the Apple Watch user population. The real-world study design has allowed for testing on many more people than are usually included in studies of a low- to moderate-risk device. Preliminary data from AHS suggest that the algorithms that will be used in the (b) (4) App results in a notification rate in the younger population that is consistent with the prevalence of AF in this population. The data also show limited numbers of adverse device effects.

Characterization of the disease

As discussed above in section 6, AF is the most common cause of stroke, and many individuals are not diagnosed with AF until the initial stroke event. Identifying AF prior to the occurrence of stroke not only will improve quality of life for those diagnosed, but will also reduce costs on the healthcare system. Given that AF can often progress in an asymptomatic manner and that this progression may be preventable through lifestyle modification, providing individuals with the ability to potentially identify AF prior to experiencing symptoms is of critical importance.

Availability of alternative treatments or diagnostics

There are no products on the market that allow for the opportunistic, background sampling accomplished by the (b) (4) App. Most individuals who will benefit from the (b) (4) App would never be given access to an Rx ECG device until after they have been diagnosed with a disease or are suspected of having the disease. By making this opportunistic, background sampling tool available more broadly, individuals may have the opportunity to learn of an important disease state before becoming symptomatic. The current standard of care for screening for AF is wrist pulse palpitation, which is infrequently carried out, and has a relatively low PPV (less than 20%).[58]

In summary, the primary benefits of the device are clear: it allows asymptomatic individuals to learn about the possible presence of AF well before such diagnosis would be made during routine clinical care. Currently, if a person is asymptomatic and not in an at-risk group, there would be no reason to screen them for AF or have them undergo an ECG, since neither are part of the standard clinical workflow. Typically, individuals are only checked for AF when they feel symptoms or when their doctor detects there may be an issue. By leveraging wearable technology that makes it easy for people to take control of their health by having the technology work seamlessly in the background, a user may learn about AF far earlier than would otherwise have occurred. By learning about possible AF early, clinicians may be able to intervene at an earlier stage to prevent longer term harm that may otherwise result from undetected AF.

As demonstrated through preliminary AHS data, the probable risks associated with use of the device are minimal, and relate primarily to anxiety that may be experienced upon learning of a possible AF diagnosis. While some individuals may delay care if they rely upon the lack of notification to indicate the absence of a medical issue, the likelihood of this occurrence is low and would require occurrence of a very specific sequence of events. Risks that are present will be mitigated against through use of the specified special controls.

Given the importance to the public's health of identifying and treating AF early, the benefits of having a device in the hands of users that will allow for earlier identification far outweigh the possible probable risks associated with the device. This benefit extends beyond users to further the clinical understanding of outcomes when AF is detected earlier, and possibly drive development of guidelines for appropriate care.

14. PROPOSED LABELING

Draft labeling (wireframes and Instructions for Use) is provided in Appendix L (wireframes) and Appendix M (draft instructions for use). Both were updated since Module 2 for clarification and response to FDA feedback. (IFU will be redlined, wireframes will not).

15. REFERENCES

[1] Ben Freedman S, Lowres N. Asymptomatic Atrial Fibrillation: The Case for Screening to Prevent Stroke. JAMA. 2015 Nov 10;314(18):1911-2.

[2] Moran PS1, Teljeur C, Ryan M, Smith SM. Systematic screening for the detection of atrial fibrillation. Cochrane Database Syst Rev. 2016 Jun 3;(6):CD009586.

[3] *See supra* note 2.

[4] Omboni S, Verberk WJ. Opportunistic screening of atrial fibrillation by automatic blood pressure measurement in the community. BMJ Open. 2016 Apr 12;6(4):e010745.

[5] *See supra* note 2.

[6] *See supra* note 1.

[7] O'Neal WT, Efird JT, Judd SE, McClure LA, Howard VJ, Howard G, Soliman EZ. Impact of Awareness and Patterns of Nonhospitalized Atrial Fibrillation on the Risk of Mortality: The Reasons for Geographic And Racial Differences in Stroke (REGARDS) Study. Clin Cardiol. 2016 Feb;39(2):103-10.

[8] *See supra* note 1.

[9] *See supra* note 2.

[10] *See supra* note 2.

[11] Brachmann J, Morillo CA, Sanna T, Di Lazzaro V, Diener HC, Bernstein RA, Rymer M, Ziegler PD, Liu S, Passman RS. Uncovering Atrial Fibrillation Beyond Short-Term Monitoring in Cryptogenic Stroke Patients: Three-Year Results From the Cryptogenic Stroke and Underlying Atrial Fibrillation Trial. Circ Arrhythm Electrophysiol. 2016 Jan;9(1):e003333.

[12] Anderson RM, Funnell MM. Patient empowerment: reflections on the challenge of fostering the adoption of a new paradigm. Patient Educ Couns. 2005 May;57(2):153–7.

[13] Melissa L, Samuel B, Jana S, Alberto C. Personal Health Records Beneficial or burdensome for patients and healthcare providers. Perspect Health Inf Manag. 2016 Spring; 13.

[14] Institute of Medicine. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC: National Academy Press; 2001.

[15] Frost & Sullivan "Market Disruption Imminent as Hospital and Physicians Aggressively Adopt Patient Portal Technology" 2013.

[16] Green, B. B., Cook, A. J., Ralston, J. D., Fishman, P. A., Catz, S. L.,Carlson, J., Carrell, D., Tyll, L., Larson, E. B., Thompson, R. S. (2008). Effectiveness of home blood pressure monitoring, Web communication, and pharmacist care on hypertension control: randomized controlled trial. Journal of the American Medical Association, 299, 2857–2867.

[17] Ralston, J. D., Hirsch, I. B., Hoath, J., Mullen, M., Cheadle, A., & Goldberg, H. I. (2009). Web-based collaborative care for Type 2 diabetes: A pilot randomized trial. Diabetes Care, 32, 234–239.

[18] Simon, G. E., Ralston, J. D., Savarino, J., Pabiniak, C., Wentzel, C., & Operskalski, B. H. (2011). Randomized trial of depression follow-up care by online messaging. Journal of General.

[19] *See supra* note 1.

[20] Lloyd-Jones DM, Wang TJ, et al. Lifetime risk for development of atrial fibrillation: the Framingham Heart Study. Circulation. 2004;110(9):1042-6.

[21] *See supra* note 20.

[22] Friberg L,Rosenqvist M, et al. High prevalence of atrial fibrillation among patients with ischemic stroke. Stroke. 2014;45(9):2599-2605.

[23] Centers for Disease Control and Prevention Atrial Fibrillation Fact Sheet. https://www.cdc.gov/dhdsp/data_statistics/fact_sheets/fs_atrial_fibrillation.htm (page last updated August 22. 2017)

[24] Colilla S, Crow A, et al. Estimates of current and future incidence and prevalence of atrial fibrillation in the U.S. adult population. Am J Cardiol. 2013;112(8):1142-7.

[25] *See supra* note 1.

[26] *See supra* note 7.

[27] Flaker GC, Belew K, et al. Asymptomatic atrial fibrillation: demographic features and prognostic information from the Atrial Fibrillation Follow-up Investigation of Rhythm Management (AFFIRM) study. Am Heart J. 2005;149(4):657-663.

[28] Tsang TS, Barnes ME, et al. Silent atrial fibrillation in Olmsted county: a community- based study. Can J Cardiol. 2011;27:S122.

[29] *See supra* note 1.

[30] Kirchof P, Benussi S, et al. 2016 ESC Guidelines for the management of atrial fibrillation developed in collaboration with EACTS. Eur Heart J. 2016;50(5):e1-e88.

[31] *See supra* note 30.

[32] Dilaveris PE, Kennedy HL. Silent atrial fibrillation: epidemiology, diagnosis, and clinical impact. Clinical Cardiology. 2017;40:413-418.

[33] Hong KL, Glover BM. The impact of lifestyle intervention on atrial fibrillation. Curr Opin Cardio. 2018;33:14-19.

[34] Turakhia MP, Shafrin J, Bognar K, et al. Economic Burden of Undiagnosed Nonvalvular Atrial Fibrillation in the United States. Am J Cardiol. 2015;116(5):733-739

[35] Sobocinski PD, Rooth ER, et al. Improved screening for silent atrial fibrillation after ischaemic stroke. Europace. 2012;14:1112-1116.

[36] Gladstone DJ, Spring M, Dorian P, et al. Atrial fibrillation in patients with cryptogenic stroke. N Engl J Med. 2014;370(26):2467-2477

[37] Reiffel JA, Verma A, et al. Incidence of Previously Undiagnosed Atrial Fibrillation Using Insertable Cardiac Monitors in a High-Risk Population The REVEAL AF Study. JAMA Cardiology. 2017;2(10):1120-1127.

[38] Wang Y, Xue H, et al. A Systematic Review of Application and Effectiveness of mHealth Interventions for Obesity and Diabetes Treatment and Self-Management. Adv Nutr. 2017;8:449-462.

[39] Miyauchi M, Toyoda M, et al. Exercise Therapy for Management of Type 2 Diabetes Mellitus: Superior Efficacy of Activity Monitors over Pedometers. Journal of Diabetes Research. 2016;5043964.

[40] Cooke G, Doust J, and Sanders S. Is pulse palpation helpful in detecting atrial fibrillation? A systematic review. The Journal of Family Practice. 2006;55(2):130-134.

[41] Chan PK, Wong CK, et al. Diagnostic performance of an automatic blood pressure measurement device, Microlife WatchBP Home A, for atrial fibrillation screening in a real-world primary care setting. BMJ Open. 2017;7:3013685.

[42] Im SI, Park DH, et al. Clinical and electrocardiographic characteristics for prediction of new-onset atrial fibrillation in asymptomatic patients with atrial premature complexes. IJC Heart & Vasculature. 2018;19:70-74.

[43] Acharya T, Tringali S, et al. Frequent atrial premature complexes and their association with risk of atrial fibrillation. American Journal of Cardiology. 2015;116:1852-1857.

[44] Katritsis DG, Zareba W, and Camm J. Nonsustained ventricular tachycardia. Journal of the American College of Cardiology. 2012;60(20):1993-2004.

[45] *See supra* note 35.

[46] *See supra* note 37.

[47] *See supra* note 32.

[48] *See supra* note 33.

[49] Aggarwal N, Selvendran S et al. Atrial fibrillation in the young: a neurologist's nightmare. Neurology Research International. 2015;2015:374352.

[50] *See supra* note 49.

[51] *See supra* note 2.

[52] *See supra* note 4.

[53] Gladstone DJ, Bui E, Fang J, et al. Potentially preventable strokes in high-risk patients with atrial fibrillation who are not adequately anticoagulated. Stroke 2009;40:235-240.

[54] *See supra* note 2.

[55] Turakhia MP, Shafrin J, Bognar K, et al. Estimated prevalence of undiagnosed atrial fibrillation in the United States Published: April 12, 2018 https://doi.org/10.1371/journal.pone. 0195088

[56] *See supra* note 2.

[57] *See supra* note 4.

[58]Jaakkola J, Vasankari T, Virtanen R, Juhani Airaksinen KE. Reliability of pulse palpation in the detection of atrial fibrillation in an elderly population. Scandinavian Journal of Primary Health Care. 2017;35(3):293-298.

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

(b)(4) - Draft

Form Approved: OMB No. 0910-0511 Expiration Date: August 31, 2019. See Instructions for OMB Statement.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
FOOD AND DRUG ADMINISTRATION
MEDICAL DEVICE USER FEE COVER SHEET

PAYMENT IDENTIFICATION NUMBER: (b) (4)
Write the Payment Identification number on your check.

A completed cover sheet must accompany each original application or supplement subject to fees. If payment is sent by U.S. mail or courier, please include a copy of this completed form with payment. Payment and mailing instructions can be found at: http://www.fda.gov/oc/mdufma/coversheet.html

1. COMPANY NAME AND ADDRESS (include name, street address, city state, country, and post office code)

Biologics Consulting Group, Inc.
1555 King St
Suite 300
Alexandria
VA
VA 22314
US

1.1 EMPLOYER IDENTIFICATION NUMBER (EIN)
*****3476

2. CONTACT NAME
Calley Herzog
2.1 E-MAIL ADDRESS
cherzog@biologicsconsulting.com
2.2 TELEPHONE NUMBER (include Area code)
720-8833633
2.3 FACSIMILE (FAX) NUMBER (Include Area code)

3. TYPE OF PREMARKET APPLICATION (Select one of the following in each column; if you are unsure, please refer to the application descriptions at the following web site: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm345263.htm

Select an application type:
[ ] Premarket notification(510(k)); except for third party
[ ] 513(g) Request for Information
[ ] Biologics License Application (BLA)
[ ] Premarket Approval Application (PMA)
[ ] Modular PMA
[ ] Product Development Protocol (PDP)
[ ] Premarket Report (PMR)
[ ] 30-Day Notice
[X] De Novo Request

3.1 Select a center
[X] CDRH
[ ] CBER

3.2 Select one of the types below
[X] Original Application

Supplement Types:
[ ] Efficacy (BLA)
[ ] Panel Track (PMA, PMR, PDP)
[ ] Real-Time (PMA, PMR, PDP)
[ ] 180-day (PMA, PMR, PDP)

4. ARE YOU A SMALL BUSINESS? (See the instructions for more information on determining this status)
[ ] YES, I meet the small business criteria and have submitted the required qualifying documents to FDA
[X] NO, I am not a small business
4.1 If Yes, please enter your Small Business Decision Number:

5. FDA WILL NOT ACCEPT YOUR SUBMISSION IF YOUR COMPANY HAS NOT PAID AN ESTABLISHMENT REGISTRATION FEE THAT IS DUE TO FDA. HAS YOUR COMPANY PAID ALL ESTABLISHMENT REGISTRATION FEES THAT ARE DUE TO FDA?
[X] YES (All of your establishments have registered and paid the fee, or this is your first device and you will register and pay the fee within 30 days after entering into an operation that requires you to register and submit device listing information.)
[ ] NO (If you currently market a medical device and your establishment is required to register and submit device listing information, FDA will not accept your submission until you have paid all fees due to FDA. See http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/RegistrationandListing/ucm053165.htm for additional information)

6. IS THIS PREMARKET APPLICATION COVERED BY ANY OF THE FOLLOWING USER FEE EXCEPTIONS? IF SO, CHECK THE APPLICABLE EXCEPTION.
[ ] This application is the first PMA submitted by a qualified small business, including any affiliates
[ ] This biologics application is submitted under section 351 of the Public Health Service Act for a product licensed for further manufacturing use only
[ ] The sole purpose of the application is to support conditions of use for a pediatric population
[ ] The application is submitted by a state or federal government entity for a device that is not to be distributed commercially

7. IS THIS A SUPPLEMENT TO A PREMARKET APPLICATION FOR WHICH FEES WERE WAIVED DUE TO SOLE USE IN A PEDIATRIC POPULATION THAT NOW PROPOSES CONDITION OF USE FOR ANY ADULT POPULATION? (If so, the application is subject to the fee that applies for an original premarket approval application (PMA).
[ ] YES [X] NO

PAPERWORK REDUCTION ACT STATEMENT
Public reporting burden for this collection of information is estimated to average 18 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing

the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the address below.

Department of Health and Human Services, Food and Drug Administration, Office of Chief Information Officer, 8455 Colesville Road, COLE-14-14253 Silver Spring, MD 20993-0002
[Please do NOT return this form to the above address, except as it pertains to comments on the burden estimate.]

8. USER FEE PAYMENT AMOUNT SUBMITTED FOR THIS PREMARKET APPLICATION

(b) (4) 31-Jul-2018

Form FDA 3601 (08/16)

"Close Window" Print Cover sheet

DEPARTMENT OF HEALTH AND HUMAN SERVICES
FOOD AND DRUG ADMINISTRATION

CDRH PREMARKET REVIEW SUBMISSION COVER SHEET

Form Approval
OMB No. 0910-0120
Expiration Date: June 30, 2020
See PRA Statement on page 5.

Date of Submission	User Fee Payment ID Number	FDA Submission Document Number *(if known)*
August 8, 2018	(b) (4)	

SECTION A TYPE OF SUBMISSION

PMA	PMA & HDE Supplement	PDP	510(k)	Request for Feedback
☐ Original Submission	☐ Regular (180 day)	☐ Original PDP	☐ Original Submission:	☐ Pre-Submission
☐ Premarket Report	☐ Special	☐ Notice of Completion	☐ Traditional	☐ Informational Meeting
☐ Modular Submission	☐ Panel Track (PMA Only)	☐ Amendment to PDP	☐ Special	☐ Submision Issue Meeting
☐ Amendment	☐ 30-day Supplement		☐ Abbreviated (Complete section I, Page 5)	☐ Day 100 Meeting
☐ Report	☐ 30-day Notice		☐ Additional Information	☐ Agreement Meeting
☐ Report Amendment	☐ 135-day Supplement		☐ Third Party	☐ Determination Meeting
☐ Licensing Agreement	☐ Real-time Review			☐ Study Risk Determination
	☐ Amendment to PMA & HDE Supplement			☐ Other *(specify):*
	☐ Other			

IDE	Humanitarian Device Exemption (HDE)	Class II Exemption Petition	Evaluation of Automatic Class III Designation (De Novo)	Other Submission
☐ Original Submission	☐ Original Submission	☐ Original Submission	☒ Original Submission	☐ 513(g)
☐ Amendment	☐ Amendment	☐ Additional Information	☐ Additional Information	☐ Other *(describe submission):*
☐ Supplement	☐ Supplement			
	☐ Report			
	☐ Report Amendment			

Have you used or cited Standards in your submission? ☐ Yes ☒ No *(If Yes, please complete Section I, Page 5)*

SECTION B SUBMITTER, APPLICANT OR SPONSOR

Company / Institution Name	Establishment Registration Number *(if known)*		
Columbia Science LLC			
Division Name *(if applicable)*	Phone Number *(including area code)*		
Street Address	FAX Number *(including area code)*		
City	State / Province	ZIP/Postal Code	Country
Contact Name			
Contact Title	Contact E-mail Address		

SECTION C APPLICATION CORRESPONDENT (e.g., consultant, if different from above)

Company / Institution Name			
Biologics Consulting Group			
Division Name *(if applicable)*	Phone Number *(including area code)*		
	410 531-6542		
Street Address	FAX Number *(including area code)*		
1555 King Street, Suite 300			
City	State / Province	ZIP Code	Country
Alexandria	VA	22314	US
Contact Name			
Donna-Bea Tillman			
Contact Title	Contact E-mail Address		
Senior Consultant	dtillman@biologicsconsulting.com		

SECTION D1 REASON FOR APPLICATION - PMA, PDP, OR HDE

- ☐ New Device
- ☐ Withdrawal
- ☐ Additional or Expanded Indications
- ☐ Request for Extension
- ☐ Post-approval Study Protocol
- ☐ Request for Applicant Hold
- ☐ Request for Removal of Applicant Hold
- ☐ Request to Remove or Add Manufacturing Site

- ☐ Process change:
  - ☐ Manufacturing ☐ Packaging
  - ☐ Sterilization
  - ☐ Other *(specify below)*

- ☐ Response to FDA correspondence:

- ☐ Change in design, component, or specification:
  - ☐ Software / Hardware
  - ☐ Color Additive
  - ☐ Material
  - ☐ Specifications
  - ☐ Other *(specify below)*

- ☐ Labeling change:
  - ☐ Indications
  - ☐ Instructions
  - ☐ Performance Characteristics
  - ☐ Shelf Life
  - ☐ Trade Name
  - ☐ Other *(specify below)*

- ☐ Location change:
  - ☐ Manufacturer
  - ☐ Sterilizer
  - ☐ Packager

- ☐ Report Submission:
  - ☐ Annual or Periodic
  - ☐ Post-approval Study
  - ☐ Adverse Reaction
  - ☐ Device Defect
  - ☐ Amendment

- ☐ Change in Ownership
- ☐ Change in Correspondent
- ☐ Change of Applicant Address

- ☐ Other Reason *(specify)*:

SECTION D2 REASON FOR APPLICATION - IDE

- ☐ New Device
- ☐ New Indication
- ☐ Addition of Institution
- ☐ Expansion / Extension of Study
- ☐ IRB Certification
- ☐ Termination of Study
- ☐ Withdrawal of Application
- ☐ Unanticipated Adverse Effect
- ☐ Notification of Emergency Use
- ☐ Compassionate Use Request
- ☐ Treatment IDE
- ☐ Continued Access

- ☐ Change in:
  - ☐ Correspondent / Applicant
  - ☐ Design / Device
  - ☐ Informed Consent
  - ☐ Manufacturer
  - ☐ Manufacturing Process
  - ☐ Protocol - Feasibility
  - ☐ Protocol - Other
  - ☐ Sponsor

- ☐ Report submission:
  - ☐ Current Investigator
  - ☐ Annual Progress Report
  - ☐ Site Waiver Report
  - ☐ Final

- ☐ Response to FDA Letter Concerning:
  - ☐ Conditional Approval
  - ☐ Deemed Approved
  - ☐ Deficient Final Report
  - ☐ Deficient Progress Report
  - ☐ Deficient Investigator Report
  - ☐ Disapproval
  - ☐ Request Extension of Time to Respond to FDA
  - ☐ Request Meeting
  - ☐ Request Hearing

- ☐ Other Reason *(specify)*:

SECTION D3 REASON FOR SUBMISSION - 510(k)

- ☐ New Device
- ☐ Additional or Expanded Indications
- ☐ Change in Technology

- ☐ Other Reason *(specify)*:

SECTION E ADDITIONAL INFORMATION ON 510(K) SUBMISSIONS

Product codes of devices to which substantial equivalence is claimed

1		2		3		4	
5		6		7		8	

Summary of, or statement concerning, safety and effectiveness information

☐ 510 (k) summary attached
☐ 510 (k) statement

Information on devices to which substantial equivalence is claimed *(if known)*

	510(k) Number		*Trade or Proprietary or Model Name*		*Manufacturer*
1		1		1	
2		2		2	
3		3		3	
4		4		4	
5		5		5	
6		6		6	

SECTION F PRODUCT INFORMATION - APPLICATION TO ALL APPLICATIONS

Common or usual name or classification name

Electrocardiograph transmitter and receiver

	Trade or Proprietary or Model Name for This Device		Model Number
1	(b) (4) App	1	
2		2	
3		3	
4		4	
5		5	

FDA document numbers of all prior related submissions *(regardless of outcome)*

1 (b)	2	3	4	5	6
7	8	9	10	11	12

Data Included in Submission

☐ Laboratory Testing ☐ Animal Trials ☐ Human Trials

SECTION G PRODUCT CLASSIFICATION - APPLICATION TO ALL APPLICATIONS

Product Code	C.F.R. Section *(if applicable)*	Device Class
DXH	21 CFR 870.2920	☐ Class I ☒ Class II ☐ Class III ☐ Unclassified

Classification Panel

Cardiovascular

Indications *(from labeling)*

See FDA Form 3881 (Appendix B)

Note: Submission of the information entered in Section H does not affect the need to submit device establishment registration.	FDA Document Number *(if known)*

SECTION H MANUFACTURING / PACKAGING / STERILIZATION SITES RELATING TO A SUBMISSION

☐ Original ☐ Add ☐ Delete	Facility Establishment Identifier (FEI) Number	☐ Manufacturer ☐ Contract Sterilizer ☐ Contract Manufacturer ☐ Repackager / Relabeler		
Company / Institution Name		Establishment Registration Number		
Division Name *(if applicable)*		Phone Number *(including area code)*		
Street Address		FAX Number *(including area code)*		
City		State / Province	ZIP Code	Country
Contact Name	Contact Title		Contact E-mail Address	

☐ Original ☐ Add ☐ Delete	Facility Establishment Identifier (FEI) Number	☐ Manufacturer ☐ Contract Sterilizer ☐ Contract Manufacturer ☐ Repackager / Relabeler		
Company / Institution Name		Establishment Registration Number		
Division Name *(if applicable)*		Phone Number *(including area code)*		
Street Address		FAX Number *(including area code)*		
City		State / Province	ZIP Code	Country
Contact Name	Contact Title		Contact E-mail Address	

☐ Original ☐ Add ☐ Delete	Facility Establishment Identifier (FEI) Number	☐ Manufacturer ☐ Contract Sterilizer ☐ Contract Manufacturer ☐ Repackager / Relabeler		
Company / Institution Name		Establishment Registration Number		
Division Name *(if applicable)*		Phone Number *(including area code)*		
Street Address		FAX Number *(including area code)*		
City		State / Province	ZIP Code	Country
Contact Name	Contact Title		Contact E-mail Address	

SECTION I — UTILIZATION OF STANDARDS

Note: Complete this section if your application or submission cites standards or includes a *"Declaration of Conformity to a Recognized Standard"* statement.

	Standards No.	Standards Organization	Standards Title	Version	Date
1					
2					
3					
4					
5					
6					
7					

Please include any additional standards to be cited on a separate page.

This section applies only to requirements of the Paperwork Reduction Act of 1995.

DO NOT SEND YOUR COMPLETED FORM TO THE PRA STAFF ADDRESS BELOW.

The burden time for this collection of information is estimated to average 0.5 hour per response, including the time to review instructions, search existing data sources, gather and maintain the data needed and complete and review the collection of information. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden, to:

Department of Health and Human Services
Food and Drug Administration
Office of Chief Information Officer
Paperwork Reduction Act (PRA) Staff
1350 Piccard Drive, Room 400
Rockville, MD 20850

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Food and Drug Administration

Indications for Use

Form Approved: OMB No. 0910-0120
Expiration Date: 06/30/2020
See PRA Statement below.

510(k) Number *(if known)*

Device Name
(b) (4) App

Indications for Use *(Describe)*
(b)(4) - Draft

[redacted]

Type of Use *(Select one or both, as applicable)*

☐ Prescription Use (Part 21 CFR 801 Subpart D) ☒ Over-The-Counter Use (21 CFR 801 Subpart C)

CONTINUE ON A SEPARATE PAGE IF NEEDED.

This section applies only to requirements of the Paperwork Reduction Act of 1995.

DO NOT SEND YOUR COMPLETED FORM TO THE PRA STAFF EMAIL ADDRESS BELOW.

The burden time for this collection of information is estimated to average 79 hours per response, including the time to review instructions, search existing data sources, gather and maintain the data needed and complete and review the collection of information. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden, to:

Department of Health and Human Services
Food and Drug Administration
Office of Chief Information Officer
Paperwork Reduction Act (PRA) Staff
PRAStaff@fda.hhs.gov

"An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB number."

Appendix C: (b) (4) Software Architecture

1. Purpose

This appendix provides the (b) (4) software architecture chart. This document also describes the high level design of the (b) (4) App, including th omponents and sub-components of the (b) (4) App and their interactions with the and operating system.

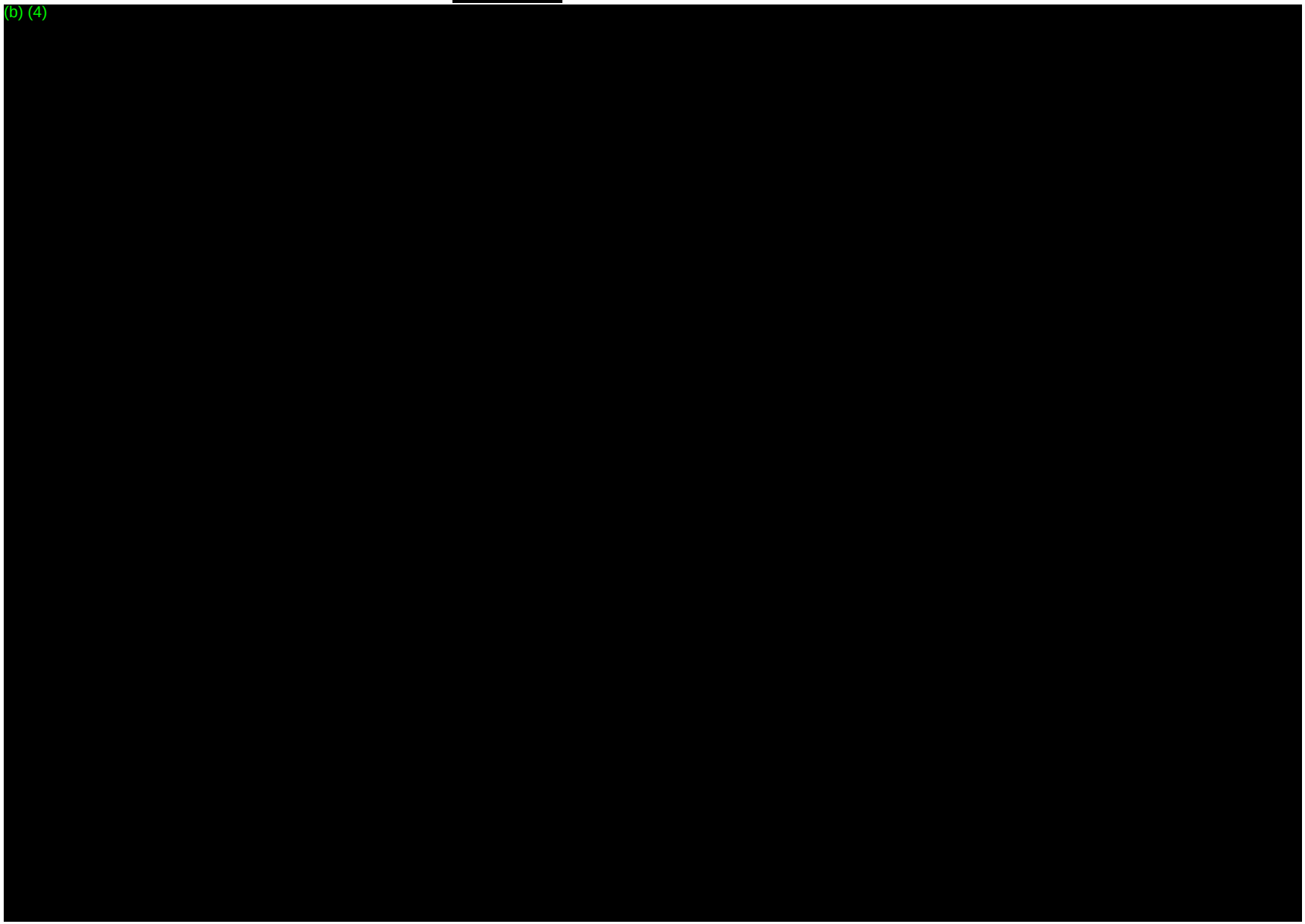
2. Definition

Term	Definition
(b) (4)	

Term	Definition
(b) (4)	

3. (b) (4) App ((b) (4) Watch and iPhone App) Architecture

4. Detailed (b) (4) Watch App Architecture/Algorithm Flow Chart



Appendix C1: (b) (4) Software Architecture (UPDATED)

1. Purpose

This appendix provides the (b) (4) software architecture chart. This document also describes the high level design of the (b) (4) App, including th omponents and sub-components of the (b) (4) App and their interactions with the and operating system.

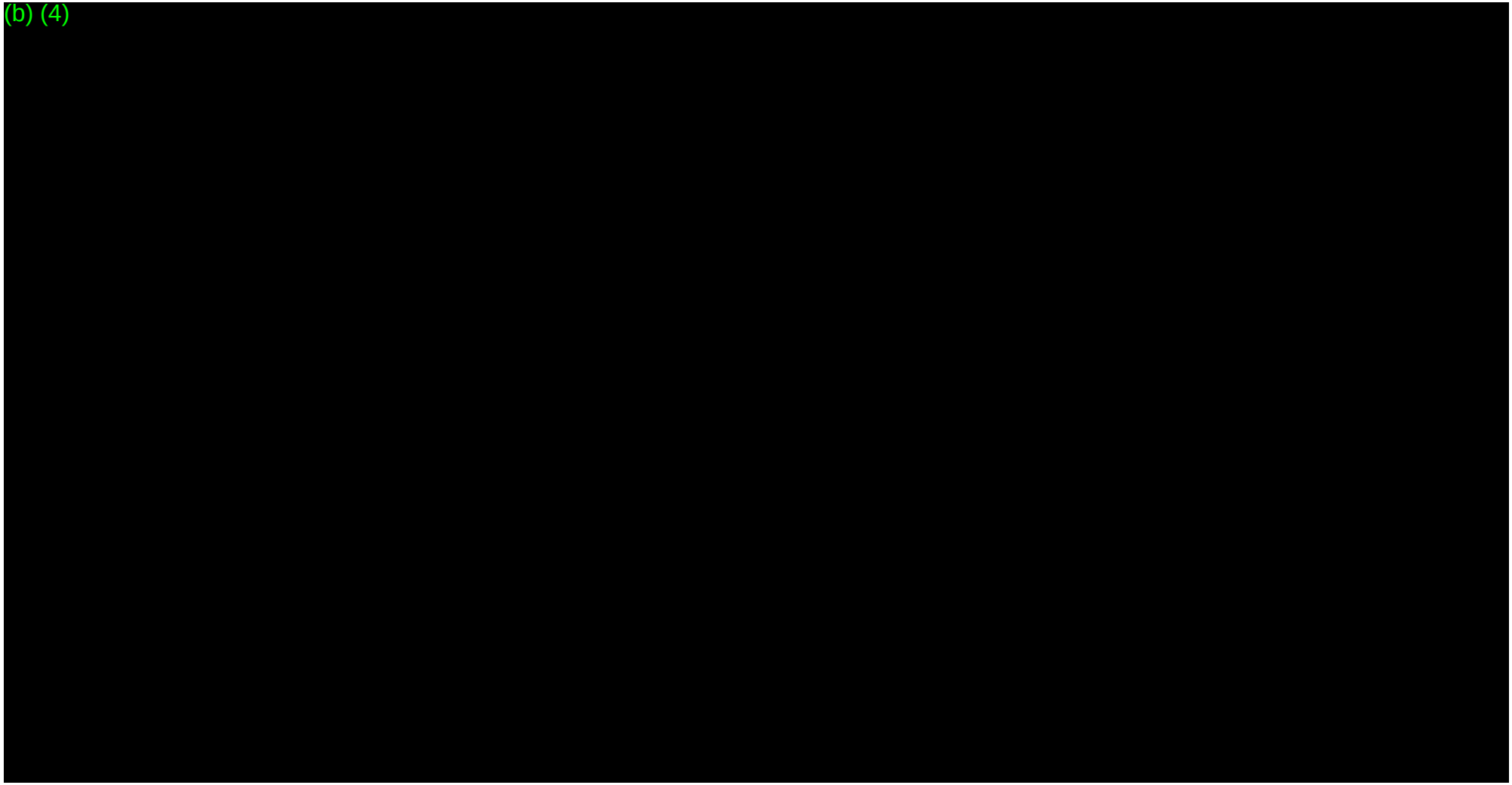
(b) (4)

2. Definition

Term	Definition
(b) (4)	

Term	Definition
(b) (4)	

3. (b) (4) App ((b) (4) Watch and iPhone App) Architecture



4. Detailed (b) (4) Watch App Architecture/Algorithm Flow Chart

(b) (4)

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Appendix F: (b)(4) Test Product and Final Product Comparison

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Appendix G: (b) (4) Off the Shelf Software

1. **What is it?** The (b) (4) App uses iOS 12.0 and watchOS 5.0 (both manufactured by Apple). iOS and watchOS both allow applications to run on them. iOS contains the Health App and iPhone HealthKit, both of which are requirements for the (b) (4) iPhone App. watchOS contains Watch HealthKit, HealthDaemon, and Health Sensor Daemon, all of which are requirements for the (b) (4) Watch App.

2. **What are the Computer System Specs for the OTS Software?** The specifications are included as part of the Software Requirements Specification provided in Appendix I.

3. **How will you assure appropriate actions are taken by the end user?** The user will need to download and install iOS 12.0 and watchOS 5.0 in order for (b) (4) on-boarding to appear and for the (b) (4) Watch App to begin analyzing tachograms and generating notifications. iOS and watchOS are typically updated on a yearly basis (major releases), and "dot" releases (minor releases) occur throughout the year.

4. **What does the OTS Software do?** iOS and watchOS allow applications to run. iOS contains the Health App, which displays health and fitness data, and iPhone HealthKit, which stores, manages, shares and sends heath and fitness data. watchOS contains Watch HealthKit which sends data to iPhone HealthKit. watchOS also contains Health Sensor Daemon, which securely transmits requests and data and HealthDaemon, which hosts (b) (4) algorithms and generation of the atrial fibrillation notification.

5. **How do you know it works?** The (b) (4) App runs on the operating system and uses features of iOS and watchOS to fulfill various requirements, so this is inherently tested through the verification testing included in Appendix O.

6. **How will you control the OTS SW?** Once the iOS kernel (core of the operating system) has started, it controls which user processes and apps can be run. To ensure that all apps come from a known and approved source and haven't been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate. Third-party apps must be validated and signed using an Apple-issued certificate. Mandatory code signing extends the concept of chain of trust from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code.

   In order to develop and install apps on iOS devices, developers must register with Apple and join the Apple Developer Program in order to be able to sign apps and submit them to the App Store for distribution. As a result, all apps in the App Store have been submitted by an identifiable person or organization, serving as a deterrent to the creation of malicious apps. They have also been reviewed by Apple to ensure they operate as described and do not contain obvious bugs or other problems.

Appendix G: (b) (4) Off the Shelf Software

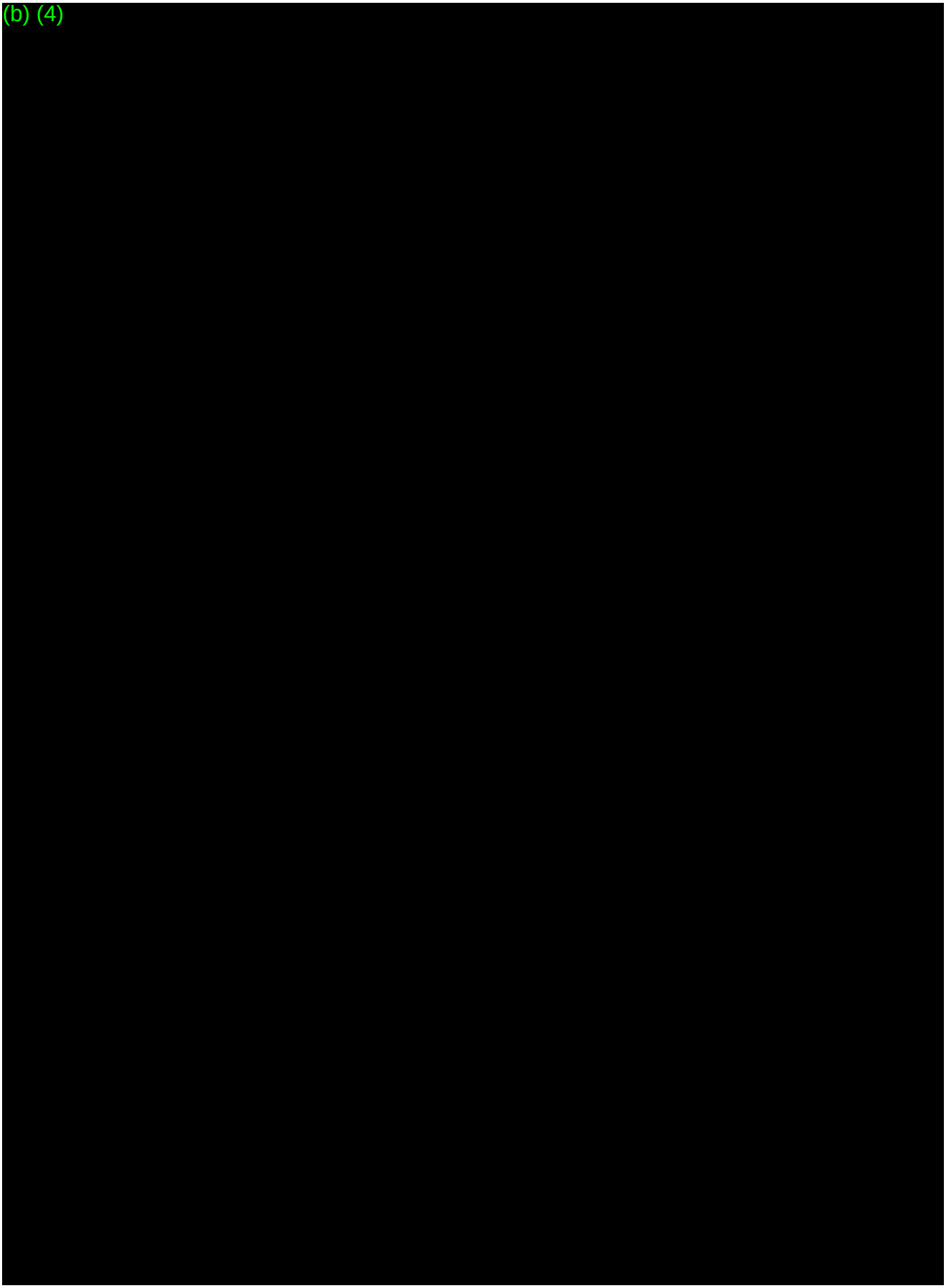
Unlike other mobile platforms, iOS doesn't allow users to install potentially malicious unsigned apps from websites, or run untrusted code. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app hasn't been modified since it was installed or last updated.

(b) (4)

(b)(4) Draft

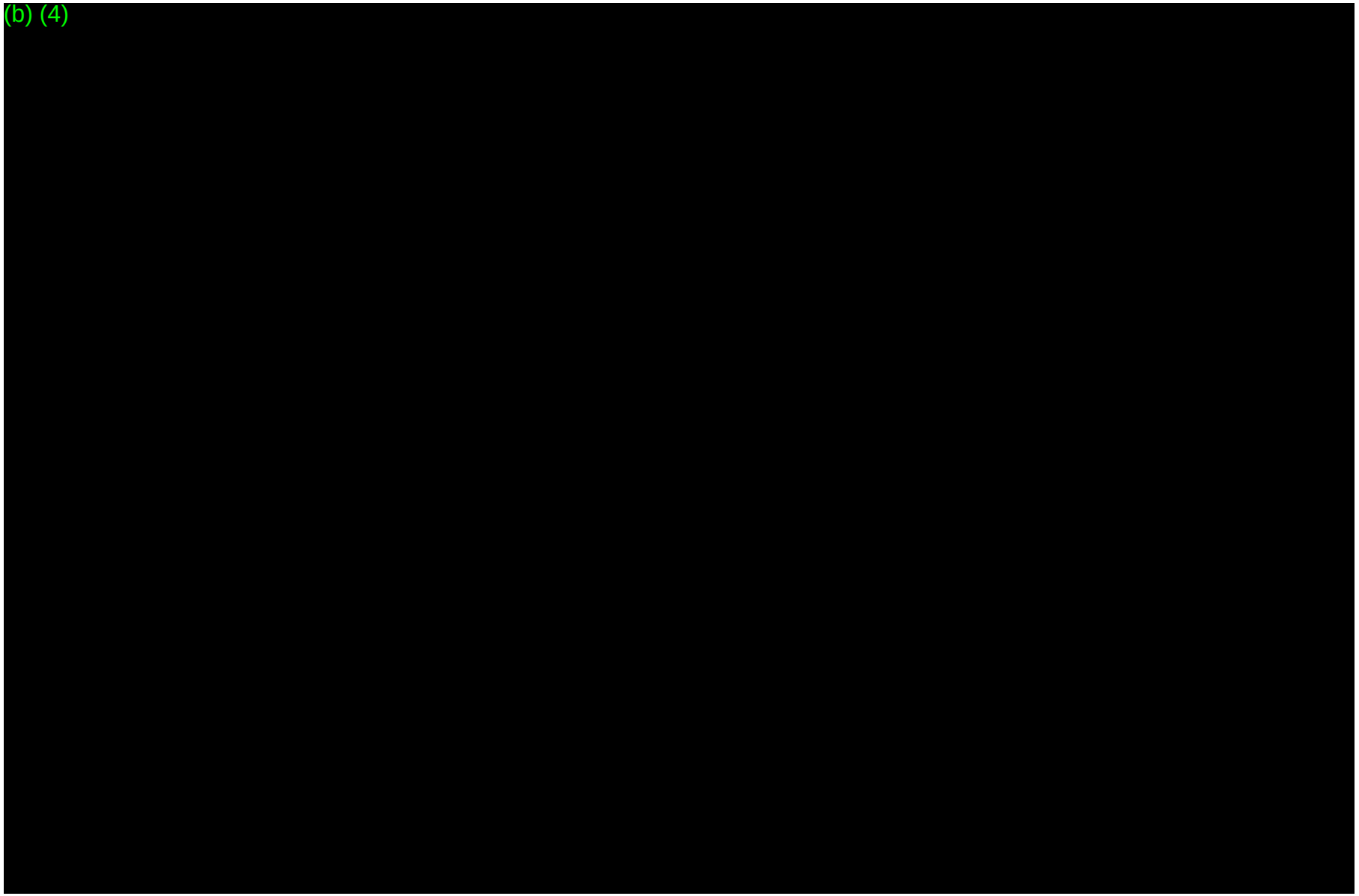
(b)(4) Draft

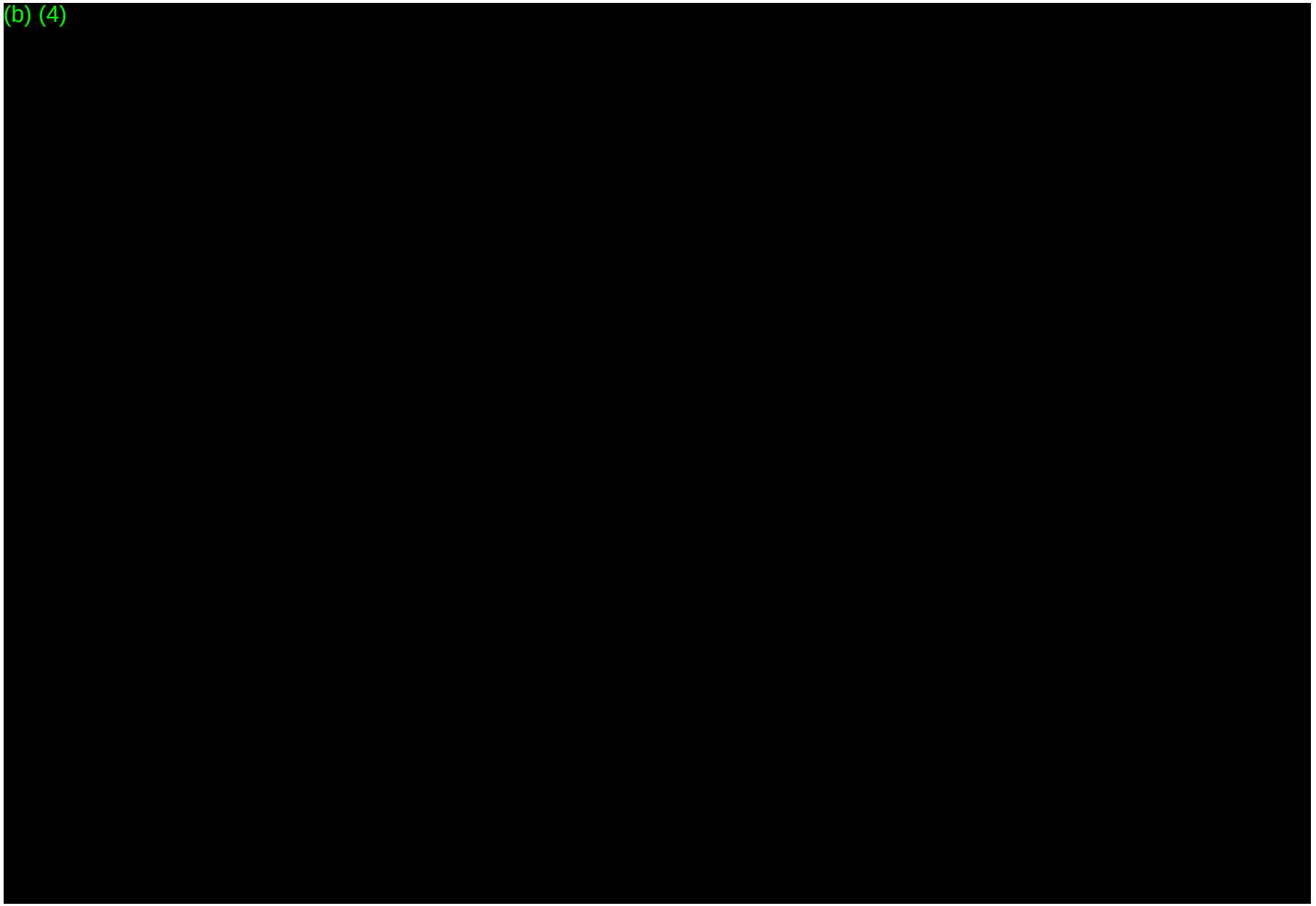
(b) (4)

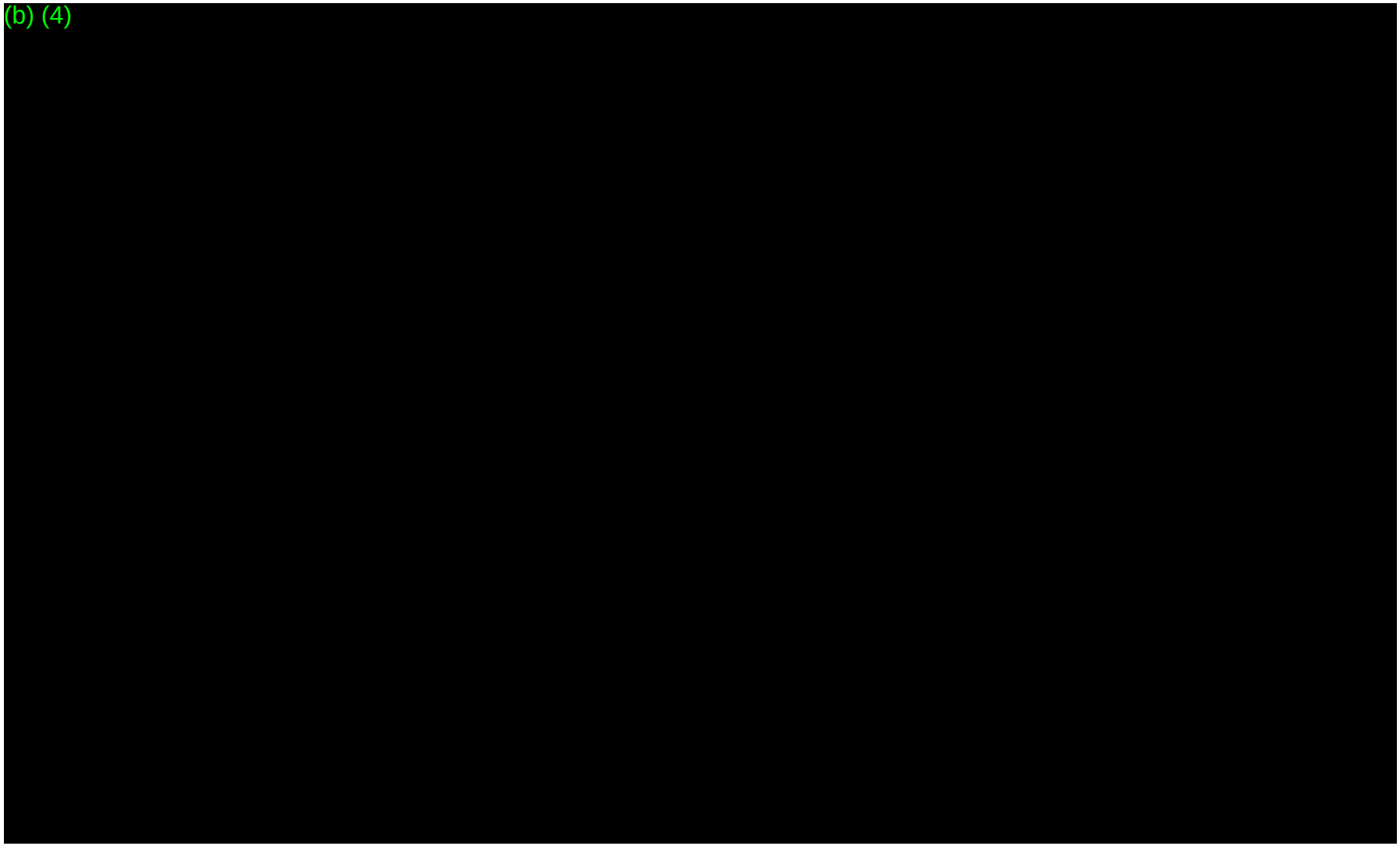


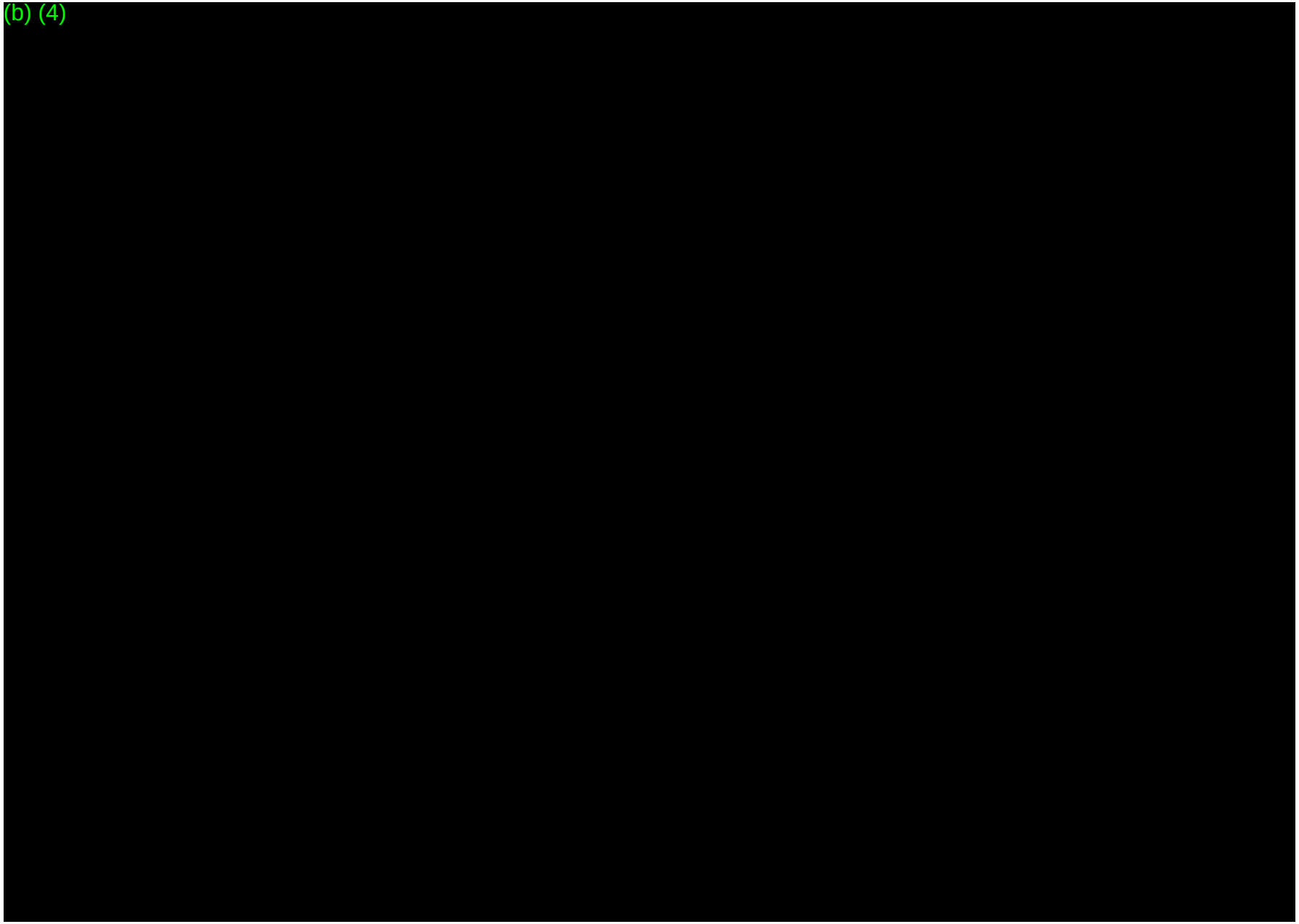
(b) (4)

(b) (4)

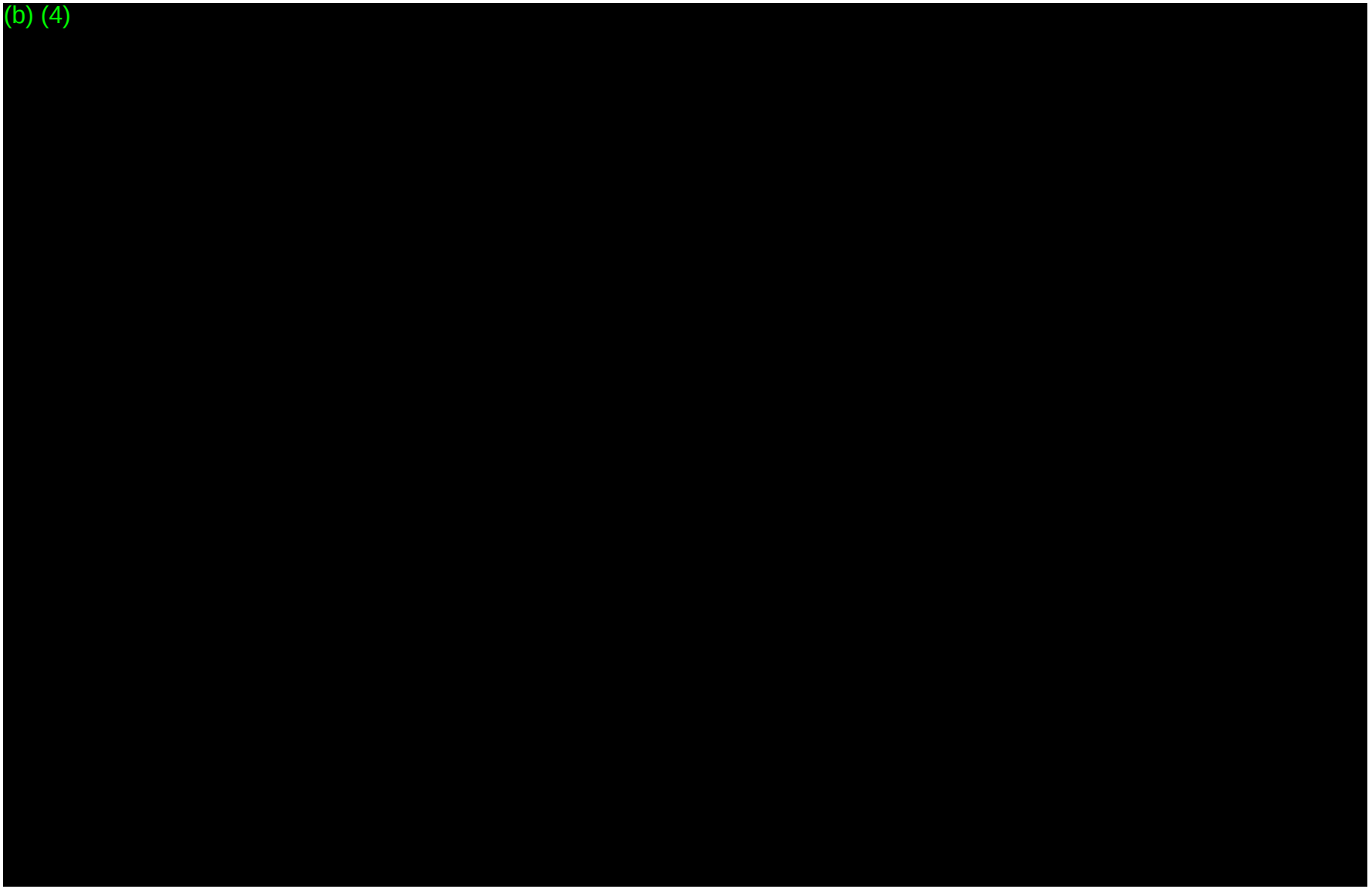






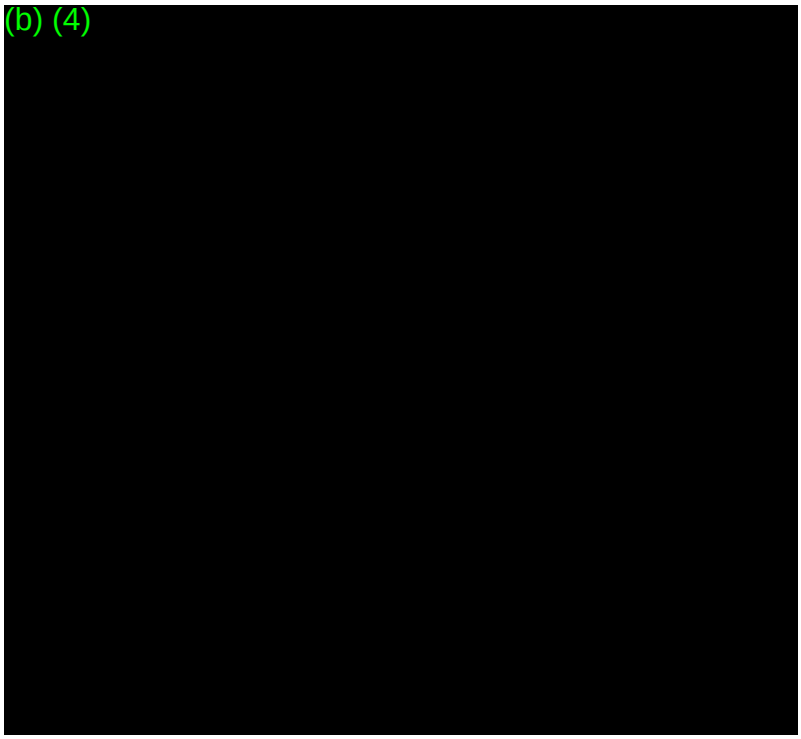


(b) (4)



Appendix H: Device Hazard Analysis

Appendix H: Device Hazard Analysis



(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

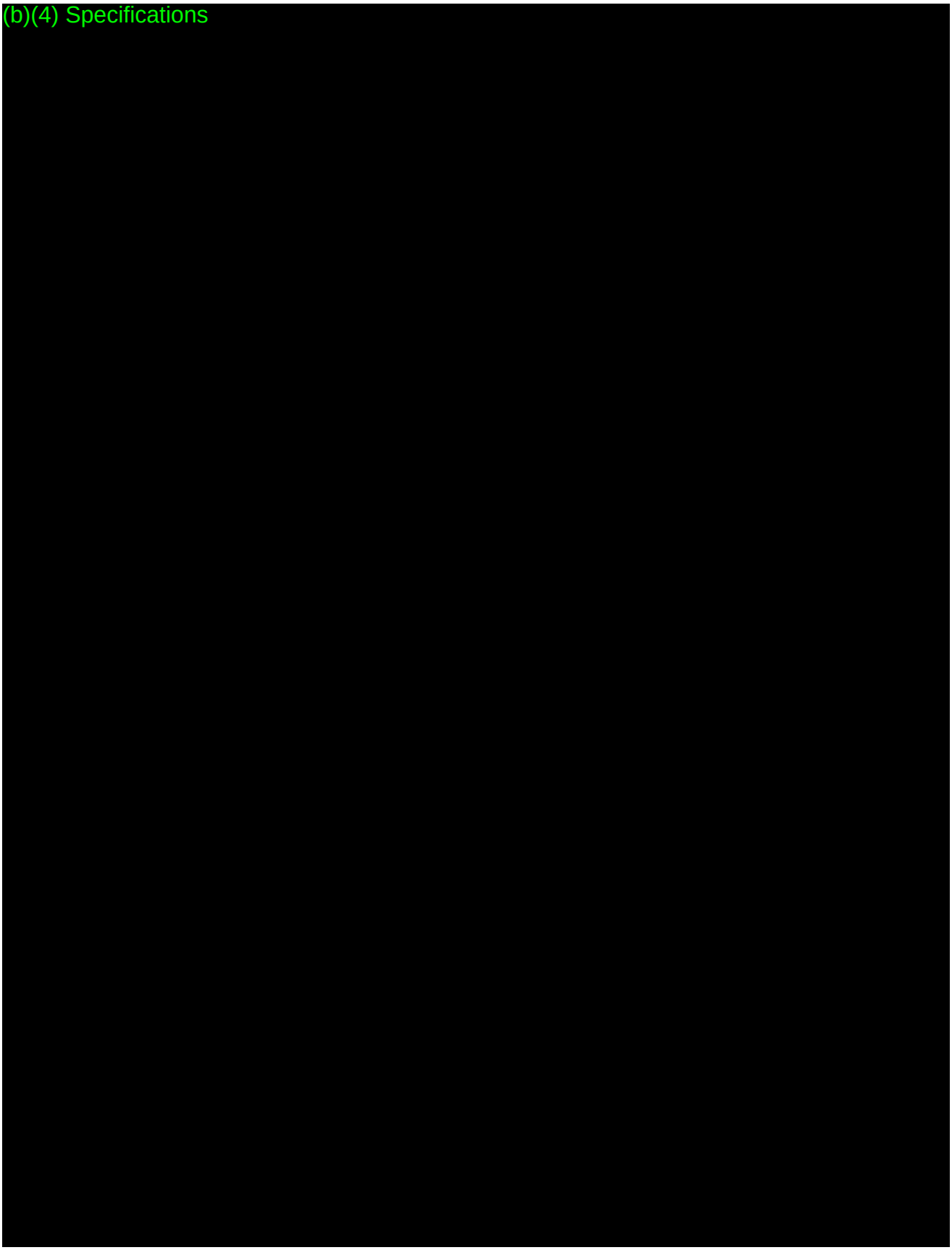
(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

Appendix I: (b) (4) Software Requirements Specification

(b)(4) Specifications



(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

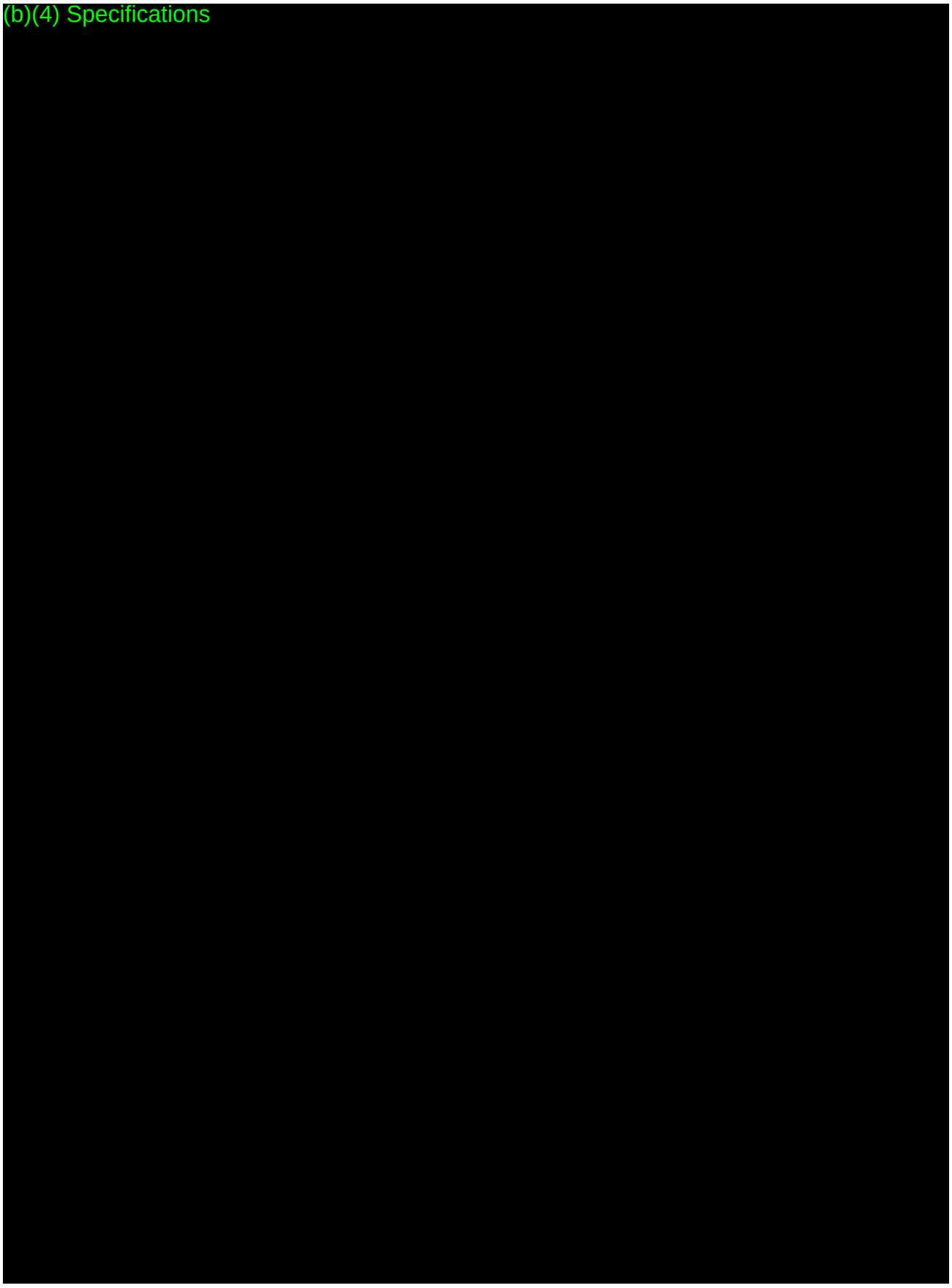
(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Specifications



(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Appendix K: (b) (4) Cybersecurity

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

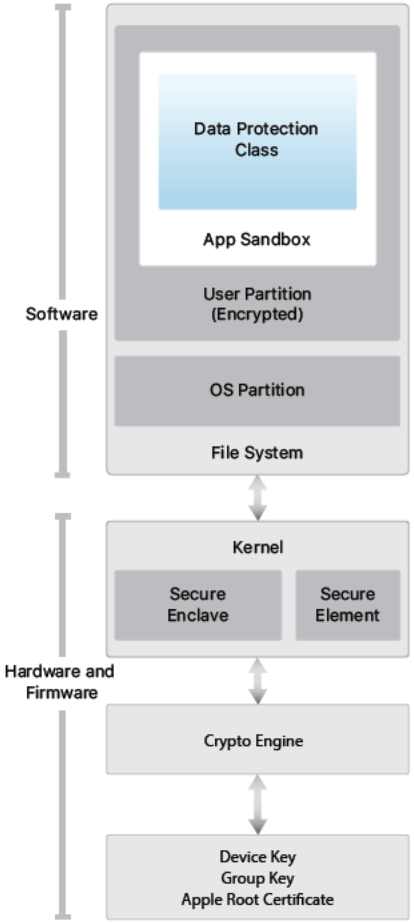
iOS Security

iOS 11

January 2018

Contents

Introduction



Security architecture diagram of iOS provides a visual overview of the different technologies discussed in this document.

Apple designed the iOS platform with security at its core. When we set out to create the best possible mobile platform, we drew from decades of experience to build an entirely new architecture. We thought about the security hazards of the desktop environment, and established a new approach to security in the design of iOS. We developed and incorporated innovative features that tighten mobile security and protect the entire system by default. As a result, iOS is a major leap forward in security for mobile devices.

Every iOS device combines software, hardware, and services designed to work together for maximum security and a transparent user experience. iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services.

iOS and iOS devices provide advanced security features, and yet they're also easy to use. Many of these features are enabled by default, so IT departments don't need to perform extensive configurations. And key security features like device encryption aren't configurable, so users can't disable them by mistake. Other features, such as Face ID, enhance the user experience by making it simpler and more intuitive to secure the device.

This document provides details about how security technology and features are implemented within the iOS platform. It will also help organizations combine iOS platform security technology and features with their own policies and procedures to meet their specific security needs.

This document is organized into the following topic areas:

- **System security:** The integrated and secure software and hardware that are the platform for iPhone, iPad, and iPod touch.
- **Encryption and data protection:** The architecture and design that protects user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.
- **App security:** The systems that enable apps to run securely and without compromising platform integrity.
- **Network security:** Industry-standard networking protocols that provide secure authentication and encryption of data in transmission.
- **Apple Pay:** Apple's implementation of secure payments.
- **Internet services:** Apple's network-based infrastructure for messaging, syncing, and backup.
- **Device controls:** Methods that allow management of iOS devices, prevent unauthorized use, and enable remote wipe if a device is lost or stolen.
- **Privacy controls:** Capabilities of iOS that can be used to control access to Location Services and user data.

System Security

Entering Device Firmware Upgrade (DFU) mode
Restoring a device after it enters DFU mode returns it to a known good state with the certainty that only unmodified Apple-signed code is present. DFU mode can be entered manually.

First connect the device to a computer using a USB cable.

Then:

On iPhone X, iPhone 8, or iPhone 8 Plus—Press and quickly release the Volume Up button. Press and quickly release the Volume Down button. Then, press and hold the side button until you see the recovery mode screen.

On iPhone 7 or iPhone 7 Plus—Press and hold the side and Volume Down buttons at the same time. Keep holding them until you see the recovery mode screen.

On iPhone 6s and earlier, iPad, or iPod touch—Press and hold both the Home and the Top (or side) buttons at the same time. Keep holding them until you see the recovery mode screen.

Note: Nothing will be displayed on the screen when the device is in DFU mode. If the Apple logo appears, the side or Sleep/Wake button was held down too long.

System security is designed so that both software and hardware are secure across all core components of every iOS device. This includes the boot-up process, software updates, and Secure Enclave. This architecture is central to security in iOS, and never gets in the way of device usability.

The tight integration of hardware, software, and services on iOS devices ensures that each component of the system is trusted, and validates the system as a whole. From initial boot-up to iOS software updates to third-party apps, each step is analyzed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly.

Secure boot chain

Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware. This secure boot chain helps ensure that the lowest levels of software aren't tampered with.

When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code, known as the hardware root of trust, is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the iBoot bootloader is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the iBoot finishes its tasks, it verifies and runs the iOS kernel. For devices with an S1, A9, or earlier A-series processor, an additional Low-Level Bootloader (LLB) stage is loaded and verified by the Boot ROM and in turn loads and verifies iBoot.

A failure of the Boot ROM to load LLB (on older devices) or iBoot (on newer devices) results in the device entering DFU mode. In the case of a failure in LLB or iBoot to load or verify the next step, startup is halted and the device displays the connect to iTunes screen. This is known as recovery mode. In either case, the device must be connected to iTunes via USB and restored to factory default settings.

On devices with cellular access, the baseband subsystem also utilizes its own similar process of secure booting with signed software and keys verified by the baseband processor.

For devices with a Secure Enclave, the Secure Enclave coprocessor also utilizes a secure boot process that ensures its separate software is verified and signed by Apple. See the "Secure Enclave" section of this paper.

For more information on manually entering recovery mode, go to: https://support.apple.com/kb/HT1808

System Software Authorization

Apple regularly releases software updates to address emerging security concerns and also provide new features; these updates are provided for all supported devices simultaneously. Users receive iOS update notifications on the device and through iTunes, and updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes.

The startup process described previously helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS uses a process called *System Software Authorization*. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS and exploit a vulnerability that's been fixed in the newer version.

On a device with Secure Enclave, the Secure Enclave coprocessor also utilizes System Software Authorization to ensure the integrity of its software and prevent downgrade installations. See the "Secure Enclave" section of this paper.

iOS software updates can be installed using iTunes or over the air (OTA) on the device. With iTunes, a full copy of iOS is downloaded and installed. OTA software updates download only the components required to complete an update, improving network efficiency, rather than downloading the entire OS. Additionally, software updates can be cached on a Mac running macOS High Sierra with Content Caching turned on, so that iOS devices don't need to redownload the necessary update over the Internet. They'll still need to contact Apple servers to complete the update process.

During an iOS upgrade, iTunes (or the device itself, in the case of OTA software updates) connects to the Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, iBoot, the kernel, and OS image), a random anti-replay value (nonce), and the device's unique ID (ECID).

The authorization server checks the presented list of measurements against versions for which installation is permitted and, if it finds a match, adds the ECID to the measurement and signs the result. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID "personalizes" the authorization for the requesting device. By authorizing and signing only for known measurements, the server ensures that the update takes place exactly as provided by Apple.

The boot-time chain-of-trust evaluation verifies that the signature comes from Apple and that the measurement of the item loaded from disk, combined with the device's ECID, matches what was covered by the signature.

These steps ensure that the authorization is for a specific device and that an old iOS version from one device can't be copied to another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software.

Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple T1, Apple S2, Apple S3, Apple A7, or later A-series processors. It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

The Secure Enclave runs an Apple-customized version of the L4 microkernel. This microkernel is signed by Apple, verified as part of the iOS secure boot chain, and updated through a personalized software update process.

When the device starts up, an ephemeral key is created, entangled with the device's UID, and used to encrypt the Secure Enclave's portion of the device's memory space. Except on the Apple A7, the Secure Enclave's memory is also authenticated with the ephemeral key. On the Apple A11, an integrity tree is used to prevent replay of security-critical Secure Enclave memory, authenticated by the ephemeral key and nonces stored in on-chip SRAM.

Additionally, data saved to the file system by the Secure Enclave is encrypted with a key entangled with the UID and an antireplay counter. Antireplay services on the Secure Enclave are used for revocation of data over events that mark antireplay boundaries including, but not limited to, the following:

- Passcode change
- Touch ID or Face ID enable/disable
- Fingerprint add/delete
- Face ID reset
- Apple Pay card add/remove
- Erase All Content and Settings

The Secure Enclave is also responsible for processing fingerprint and face data from the Touch ID and Face ID sensors, determining if there's a match, and then enabling access or purchases on behalf of the user.

Touch ID

Touch ID is the fingerprint sensing system that makes secure access to iPhone and iPad faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

Face ID

With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing, so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data.

Touch ID, Face ID, and passcodes

To use Touch ID or Face ID, you must set up your device so that a passcode is required to unlock it. When Touch ID or Face ID detects a successful match, your device unlocks without asking for the device passcode. This makes using a longer, more complex passcode far more practical because you don't need to enter it as frequently. Touch ID and Face ID don't replace your passcode, but provide easy access to your device within thoughtful boundaries and time constraints. This is important because a strong passcode forms the foundation of your iOS device's cryptographic protection.

You can always use your passcode instead of Touch ID or Face ID, and it's still required under the following circumstances:

- The device has just been turned on or restarted.
- The device hasn't been unlocked for more than 48 hours.
- The passcode hasn't been used to unlock the device in the last 156 hours (six and a half days) and Face ID hasn't unlocked the device in the last 4 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match.
- After initiating power off/Emergency SOS.

When Touch ID or Face ID is enabled, the device immediately locks when the side button is pressed, and the device locks every time it goes to sleep. Touch ID and Face ID require a successful match—or optionally the passcode—at every wake.

The probability that a random person in the population could look at your iPhone X and unlock it using Face ID is approximately 1 in 1,000,000 (versus 1 in 50,000 for Touch ID). For additional protection, both Touch ID and Face ID allow only five unsuccessful match attempts before a passcode is required to obtain access to your device. With Face ID, the probability of a false match is different for twins and siblings that look like you as well as among children under the age of 13, because their distinct facial features may not have fully developed. If you're concerned about this, Apple recommends using a passcode to authenticate.

Touch ID security

The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but can't read it. It's encrypted and authenticated with a session key that is negotiated using a shared key provisioned for each Touch ID sensor and its corresponding Secure Enclave at the factory. The shared key is strong, random, and different for every Touch ID sensor. The session key exchange uses AES key wrapping with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption.

The raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map

of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes.

Face ID security

Face ID is designed to confirm user attention, provide robust authentication with a low false match rate, and mitigate both digital and physical spoofing.

The TrueDepth camera automatically looks for your face when you wake iPhone X by raising it or tapping the screen, as well as when iPhone X attempts to authenticate you to display an incoming notification or when a supported app requests Face ID authentication. When a face is detected, Face ID confirms attention and intent to unlock by detecting that your eyes are open and directed at your device; for accessibility, this is disabled when VoiceOver is activated and, if required, can be disabled separately.

Once it confirms the presence of an attentive face, the TrueDepth camera projects and reads over 30,000 infrared dots to form a depth map of the face, along with a 2D infrared image. This data is used to create a sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave. To counter both digital and physical spoofs, the TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern. A portion of the A11 Bionic chip's neural engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of your face captured across a variety of poses.

Facial matching is performed within the Secure Enclave using neural networks trained specifically for that purpose. We developed the facial matching neural networks using over a billion images, including IR and depth images collected in studies conducted with the participants' informed consent. Apple worked with participants from around the world to include a representative group of people accounting for gender, age, ethnicity, and other factors. The studies were augmented as needed to provide a high degree of accuracy for a diverse range of users. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. An additional neural network that's trained to spot and resist spoofing defends against attempts to unlock your iPhone X with photos or masks.

Face ID data, including mathematical representations of your face, is encrypted and available only to the Secure Enclave. This data never leaves the device. It isn't sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation:

- The mathematical representations of your face calculated during enrollment.
- The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching.

Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data.

How Touch ID or Face ID unlocks an iOS device

With Touch ID or Face ID disabled, when a device locks, the keys for the highest class of Data Protection—which are held in the Secure Enclave—are discarded. The files and Keychain items in that class are inaccessible until you unlock the device by entering your passcode.

With Touch ID or Face ID enabled, the keys aren't discarded when the device locks; instead, they're wrapped with a key that's given to the Touch ID or Face ID subsystem inside the Secure Enclave. When you attempt to unlock the device, if the device detects a successful match, it provides the key for unwrapping the Data Protection keys, and the device is unlocked. This process provides additional protection by requiring cooperation between the Data Protection and Touch ID or Face ID subsystems to unlock the device.

When the device restarts, the keys required for Touch ID or Face ID to unlock the device are lost; they're discarded by the Secure Enclave after any conditions are met that require passcode entry (for example, after not being unlocked for 48 hours or after five failed match attempts).

To improve unlock performance and keep pace with the natural changes of your face and look, Face ID augments its stored mathematical representation over time. Upon successful unlock, Face ID may use the newly calculated mathematical representation—if its quality is sufficient—for a finite number of additional unlocks before that data is discarded. Conversely, if Face ID fails to recognize you, but the match quality is higher than a certain threshold and you immediately follow the failure by entering your passcode, Face ID takes another capture and augments its enrolled Face ID data with the newly calculated mathematical representation. This new Face ID data is discarded if you stop matching against it and after a finite number of unlocks. These augmentation processes allow Face ID to keep up with dramatic changes in your facial hair or makeup use, while minimizing false acceptance.

Touch ID, Face ID, and Apple Pay

You can also use Touch ID and Face ID with Apple Pay to make easy and secure purchases in stores, apps, and on the web. For more information on Touch ID and Apple Pay, see the Apple Pay section of this paper.

To authorize an in-store payment with Face ID, you must first confirm intent to pay by double-clicking the side button. You then authenticate using Face ID before placing your iPhone X near the contactless payment reader. If you'd like to select a different Apple Pay payment method after Face ID authentication, you'll need to reauthenticate, but you won't have to double-click the side button again.

To make a payment within apps and on the web, you confirm intent to pay by double-clicking the side button, then authenticate using Face ID to authorize the payment. If your Apple Pay transaction isn't completed within 30 seconds of double-clicking the side button, you'll have to reconfirm intent to pay by double-clicking again.

Face ID Diagnostics

Face ID data doesn't leave your device, and is never backed up to iCloud or anywhere else. Only in the case that you wish to provide Face ID diagnostic data to AppleCare for support will this information be transferred from your device. Enabling Face ID Diagnostics requires a digitally signed authorization from Apple that's similar to the one used in the software update personalization process. After authorization, you'll be able to activate Face ID Diagnostics and begin the setup process from within the Settings app of your iPhone X.

As part of setting up Face ID Diagnostics, your existing Face ID enrollment will be deleted and you'll be asked to re-enroll in Face ID. Your iPhone X will begin recording Face ID images captured during authentication attempts for the next 10 days; iPhone X will automatically stop saving images thereafter. Face ID Diagnostics doesn't automatically send data to Apple. You can review and approve Face ID Diagnostics data—including enrollment and unlock images (both failed and successful) that are gathered while in diagnostics mode—before it's sent to Apple. Face ID Diagnostics will upload only the Face ID Diagnostics images you have approved, the data is encrypted before it's uploaded, and is immediately deleted from your iPhone X after the upload completes. Images you reject are immediately deleted.

If you don't conclude the Face ID Diagnostics session by reviewing images and uploading any approved images, Face ID Diagnostics will automatically end after 40 days, and all diagnostic images will be deleted from your iPhone X. You can also disable Face ID Diagnostics at any time. All local images are immediately deleted if you do so, and no Face ID data is shared with Apple in these cases.

Other uses for Touch ID and Face ID

Third-party apps can use system-provided APIs to ask the user to authenticate using Touch ID or Face ID or a passcode, and apps that support Touch ID automatically support Face ID without any changes. When using Touch ID or Face ID, the app is notified only as to whether the authentication was successful; it can't access Touch ID, Face ID, or the data associated with the enrolled user. Keychain items can also be protected with Touch ID or Face ID, to be released by the Secure Enclave only by a successful match or the device passcode. App developers have APIs to verify that a passcode has been set by the user, before requiring Touch ID or Face ID or a passcode to unlock Keychain items. App developers can do the following:

- Require that authentication API operations don't fall back to an app password or the device passcode. They can query whether a user is enrolled, allowing Touch ID or Face ID to be used as a second factor in security-sensitive apps.
- Generate and use ECC keys inside Secure Enclave that can be protected by Touch ID or Face ID. Operations with these keys are always performed inside the Secure Enclave once it authorizes their use.

You can also configure Touch ID or Face ID to approve purchases from the iTunes Store, the App Store, and the iBooks Store, so you don't have to enter an Apple ID password. With iOS 11 or later, Touch ID– and Face ID–protected Secure Enclave ECC keys are used to authorize a purchase by signing the store request.

Encryption and Data Protection

Erase All Content and Settings
The "Erase all content and settings" option in Settings obliterates all the keys in Effaceable Storage, rendering all user data on the device cryptographically inaccessible. Therefore, it's an ideal way to be sure all personal information is removed from a device before giving it to somebody else or returning it for service.

Important: Don't use the "Erase all content and settings" option until device has been backed up, as there is no way to recover the erased data.

The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run on a device. iOS has additional encryption and data protection features to safeguard user data, even in cases where other parts of the security infrastructure have been compromised (for example, on a device with unauthorized modifications). This provides important benefits for both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

Hardware security features

On mobile devices, speed and power efficiency are critical. Cryptographic operations are complex and can introduce performance or battery life problems if not designed and implemented with these priorities in mind.

Every iOS device has a dedicated AES-256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient. On A9 or later A-series processors, the flash storage subsystem is on an isolated bus that is only granted access to memory containing user data via the DMA crypto engine.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused (UID) or compiled (GID) into the application processor and Secure Enclave during manufacturing. No software or firmware can read them directly; they can see only the results of encryption or decryption operations performed by dedicated AES engines implemented in silicon using the UID or GID as a key. Additionally, the Secure Enclave's UID and GID can only be used by the AES engine dedicated to the Secure Enclave. The UIDs and GIDs are also not available via JTAG or other debugging interfaces.

On T1, S2, S3, and A9 or later A-series processors, each Secure Enclave generates its own UID (Unique ID). Because the UID is unique to each device, and because it is generated wholly within the Secure Enclave instead of in a manufacturing system outside of the device, the UID is not available for access or storage by Apple or any of its suppliers. Software running on the Secure Enclave takes advantage of the UID to protect device-specific secrets.

The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID isn't related to any other identifier on the device.

The GID is common to all processors in a class of devices (for example, all devices using the Apple A8 processor).

Apart from the UID and GID, all other cryptographic keys are created by the system's random number generator (RNG) using an algorithm based on CTR_DRBG. System entropy is generated from timing variations during

boot, and additionally from interrupt timing once the device has booted. Keys generated inside the Secure Enclave use its true hardware random number generator based on multiple ring oscillators post processed with CTR_DRBG.

Securely erasing saved keys is just as important as generating them. It's especially challenging to do so on flash storage, for example, wear-leveling might mean multiple copies of data need to be erased. To address this issue, iOS devices include a feature dedicated to secure data erasure called *Effaceable Storage*. This feature accesses the underlying storage technology (for example, NAND) to directly address and erase a small number of blocks at a very low level.

File Data Protection

In addition to the hardware encryption features built into iOS devices, Apple uses a technology called *Data Protection* to further protect data stored in flash memory on the device. Data Protection allows the device to respond to common events such as incoming phone calls, but also enables a high level of encryption for user data. Key system apps, such as Messages, Mail, Calendar, Contacts, Photos, and Health data values use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically.

Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device. Data Protection is controlled on a per-file basis by assigning each file to a class; accessibility is determined by whether the class keys have been unlocked. With the advent of the Apple File System (APFS), the file system is now able to further sub-divide the keys into a per-extent basis (portions of a file can have different keys).

Architecture overview

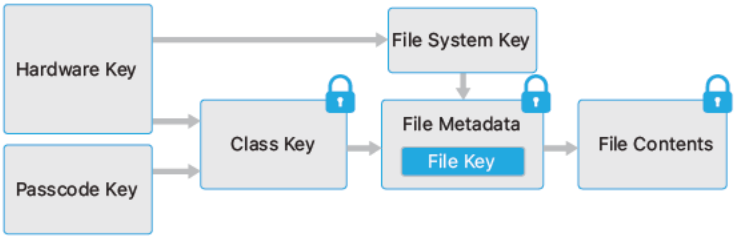
Every time a file on the data partition is created, Data Protection creates a new 256-bit key (the "per-file" key) and gives it to the hardware AES engine, which uses the key to encrypt the file as it is written to flash memory using AES CBC mode. (On devices with an A8 or later processor, AES-XTS is used.) The initialization vector (IV) is calculated with the block offset into the file, encrypted with the SHA-1 hash of the per-file key.

The per-file (or per-extent) key is wrapped with one of several class keys, depending on the circumstances under which the file should be accessible. Like all other wrappings, this is performed using NIST AES key wrapping, per RFC 3394. The wrapped per-file key is stored in the file's metadata.

Devices running with the Apple File System format may support cloning of files (zero-cost copies using copy-on-write technology). If a file is cloned, each half of the clone gets a new key to accept incoming writes so that new data is written to the media with a new key. Over time, the file may become composed of various extents (or fragments), each mapping to different keys. However, all of the extents that comprise a file will be guarded by the same class key.

When a file is opened, its metadata is decrypted with the file system key, revealing the wrapped per-file key and a notation on which class protects it. The per-file (or per-extent) key is unwrapped with the class key, then supplied to the hardware AES engine, which decrypts the file as it is read from flash memory. All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the application processor. At boot, the Secure Enclave negotiates an ephemeral key with the AES engine. When the Secure Enclave unwraps a file's keys, they are rewrapped with the ephemeral key and sent back to the application processor.

The metadata of all files in the file system is encrypted with a random key, which is created when iOS is first installed or when the device is wiped by a user. On devices that support the Apple File System, the file system metadata key is wrapped by the Secure Enclave UID key for long-term storage. Just like per-file or per-extent keys, the metadata key is never directly exposed to the application processor; the Secure Enclave provides an ephemeral, per-boot version instead. When stored, the encrypted file system key is additionally wrapped by an "effaceable key" stored in Effaceable Storage. This key does not provide additional confidentiality of data. Instead, it's designed to be quickly erased on demand (by the user with the "Erase All Content and Settings" option, or by a user or administrator issuing a remote wipe command from an MDM solution, Exchange ActiveSync, or iCloud). Erasing the key in this manner renders all files cryptographically inaccessible.



The content of a file may be encrypted with one or more per-file (or per-extent) keys that are wrapped with a class key and stored in a file's metadata, which in turn is encrypted with the file system key. The class key is protected with the hardware UID and, for some classes, the user's passcode. This hierarchy provides both flexibility and performance. For example, changing a file's class only requires rewrapping its per-file key, and a change of passcode just rewraps the class key.

Passcodes

Passcode considerations
If a long password that contains only numbers is entered, a numeric keypad is displayed at the Lock screen instead of the full keyboard. A longer numeric passcode may be easier to enter than a shorter alphanumeric passcode, while providing similar security.

By setting up a device passcode, the user automatically enables Data Protection. iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. This means an attacker in possession of a device can't get access to data in specific protection classes without the passcode.

The passcode is entangled with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than five and a half years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

Delays between passcode attempts

Attempts	Delay Enforced
1–4	none
5	1 minute
6	5 minutes
7–8	15 minutes
9	1 hour

The stronger the user passcode is, the stronger the encryption key becomes. Touch ID and Face ID can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection, without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day.

To further discourage brute-force passcode attacks, there are escalating time delays after the entry of an invalid passcode at the Lock screen. If Settings > Touch ID & Passcode > Erase Data is turned on, the device will automatically wipe after 10 consecutive incorrect attempts to enter the passcode. This setting is also available as an administrative policy through MDM and Exchange ActiveSync, and can be set to a lower threshold.

On devices with Secure Enclave, the delays are enforced by the Secure Enclave coprocessor. If the device is restarted during a timed delay, the delay is still enforced, with the timer starting over for the current period.

Data Protection classes

When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible. The basic classes and policies are described in the following sections.

Complete Protection

(`NSFileProtectionComplete`): The class key is protected with a key derived from the user passcode and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID or Face ID.

Protected Unless Open

(`NSFileProtectionCompleteUnlessOpen`): Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behavior is achieved by using asymmetric elliptic curve cryptography (ECDH over Curve25519). The usual per-file key is protected by a key derived using One-Pass Diffie-Hellman Key Agreement as described in NIST SP 800-56A.

The ephemeral public key for the agreement is stored alongside the wrapped per-file key. The KDF is Concatenation Key Derivation Function (Approved Alternative 1) as described in 5.8.1 of NIST SP 800-56A. AlgorithmID is omitted. PartyUInfo and PartyVInfo are the ephemeral and static public keys, respectively. SHA-256 is used as the hashing function. As soon as the file is closed, the per-file key is wiped from memory. To open the file again, the shared secret is re-created using the Protected Unless Open class's private key and the file's ephemeral public key, which are used to unwrap the per-file key that is then used to decrypt the file.

Protected Until First User Authentication

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): This class behaves in the same way as Complete Protection, except that the decrypted class key isn't removed from memory when the device is locked. The protection in this class has similar properties to desktop full-volume encryption, and protects data from attacks that involve a reboot. This is the default class for all third-party app data not otherwise assigned to a Data Protection class.

No Protection

(`NSFileProtectionNone`): This class key is protected only with the UID, and is kept in Effaceable Storage. Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe. If a file isn't assigned a Data Protection class, it is still stored in encrypted form (as is all data on an iOS device).

Data protection class key

Class A Complete Protection	(NSFileProtectionComplete)
Class B Protected Unless Open	(NSFileProtectionCompleteUnlessOpen)
Class C Protected Until First User Authentication	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Class D No Protection	(NSFileProtectionNone)

Keychain Data Protection

Many apps need to handle passwords and other short but sensitive bits of data, such as keys and login tokens. The iOS Keychain provides a secure way to store these items.

The Keychain is implemented as a SQLite database stored on the file system. There is only one database and the *securityd* daemon determines which Keychain items each process or apps can access. Keychain access APIs result in calls to the daemon, which queries the app's "Keychain-access-groups," "application-identifier," and "application-group" entitlements. Rather than limiting access to a single process, access groups allow Keychain items to be shared between apps.

Keychain items can only be shared between apps from the same developer. This is managed by requiring third-party apps to use access groups with a prefix allocated to them through the Apple Developer Program via application groups. The prefix requirement and application group uniqueness are enforced through code signing, Provisioning Profiles, and the Apple Developer Program.

Keychain data is protected using a class structure similar to the one used in file Data Protection. These classes have behaviors equivalent to file Data Protection classes, but use distinct keys and are part of APIs that are named differently.

Availability	File Data Protection	Keychain Data Protection
When unlocked	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways
Passcode enabled	N/A	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

Apps that utilize background refresh services can use `kSecAttrAccessibleAfterFirstUnlock` for Keychain items that need to be accessed during background updates.

The class `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` behaves the same as `kSecAttrAccessibleWhenUnlocked`; however, it is only available when the device is configured with a passcode. This class exists only in the system keybag; they don't sync to iCloud Keychain, aren't backed up, and aren't included in escrow keybags. If the passcode is removed or reset, the items are rendered useless by discarding the class keys.

Other Keychain classes have a "This device only" counterpart, which is always protected with the UID when being copied from the device during a backup, rendering it useless if restored to a different device.

Apple has carefully balanced security and usability by choosing Keychain classes that depend on the type of information being secured and when it's needed by iOS. For example, a VPN certificate must always be available so the device keeps a continuous connection, but it's classified as "non-migratory," so it can't be moved to another device.

Components of a Keychain item

Along with the access group, each Keychain item contains administrative metadata (such as "created" and "last updated" timestamps).

It also contains SHA-1 hashes of the attributes used to query for the item (such as the account and server name) to allow lookup without decrypting each item. And finally, it contains the encryption data, which includes the following:

- Version number
- Access control list (ACL) data
- Value indicating which protection class the item is in
- Per-item key wrapped with the protection class key
- Dictionary of attributes describing the item (as passed to SecItemAdd), encoded as a binary plist and encrypted with the per-item key

The encryption is AES 128 in GCM (Galois/Counter Mode); the access group is included in the attributes and protected by the GMAC tag calculated during encryption.

For Keychain items created by iOS, the following class protections are enforced:

Item	Accessible
Wi-Fi passwords	After first unlock
Mail accounts	After first unlock
Exchange accounts	After first unlock
VPN passwords	After first unlock
LDAP, CalDAV, CardDAV	After first unlock
Social network account tokens	After first unlock
Handoff advertisement encryption keys	After first unlock
iCloud token	After first unlock
Home sharing password	When unlocked
Find My iPhone token	Always
Voicemail	Always
iTunes backup	When unlocked, non-migratory
Safari passwords	When unlocked
Safari bookmarks	When unlocked
VPN certificates	Always, non-migratory
Bluetooth® keys	Always, non-migratory
Apple Push Notification service token	Always, non-migratory
iCloud certificates and private key	Always, non-migratory
iMessage keys	Always, non-migratory
Certificates and private keys installed by a configuration profile	Always, non-migratory
SIM PIN	Always, non-migratory

Keychain access control

Keychains can use access control lists (ACLs) to set policies for accessibility and authentication requirements. Items can establish conditions that require user presence by specifying that they can't be accessed unless authenticated using Touch ID, Face ID, or by entering the device's passcode. Access to items can also be limited by specifying that Touch ID or Face ID enrollment hasn't changed since the item was added. This limitation helps prevent an attacker from adding their own fingerprint in order to access a Keychain item. ACLs are evaluated inside the Secure Enclave and are released to the kernel only if their specified constraints are met.

Access to Safari saved passwords

iOS apps can interact with Keychain items saved by Safari for Password AutoFill using the following two APIs:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Access is granted only if both the app developer and website administrator have given their approval, and the user has given consent. App developers express their intent to access Safari saved passwords by including an entitlement in their app. The entitlement lists the fully qualified domain names of associated websites. The websites must place a file on their server listing the unique app identifiers of apps they've approved. When an app with the com.apple.developer.associated-domains entitlement is installed, iOS makes a TLS request to each listed website, requesting the file/apple-app-site-association. If the file lists the app identifier of the app being installed, then iOS marks the website and app as having a trusted relationship. Only with a trusted relationship will calls to these two APIs result in a prompt to the user, who must agree before any passwords are released to the app, or are updated or deleted.

iOS allows users to input saved user names and passwords into credential-related fields in apps by tapping a "key" affordance in the iOS keyboard's QuickType bar. It leverage the same apple-app-site-association mechanism to strongly associate apps and websites. This interface exposes no credential information to the app until a user consents to releasing a credential to the app. When iOS has marked a website and app as having a trusted relationship, the QuickType bar will also directly suggest credentials to fill into the app. This allows users to choose to disclose Safari-saved credentials to apps with the same security story, but without apps having to adopt an API.

Keybags

The keys for both file and Keychain Data Protection classes are collected and managed in keybags. iOS uses the following keybags: user, device, backup, escrow, and iCloud Backup.

User keybag is where the wrapped class keys used in normal operation of the device are stored. For example, when a passcode is entered, the `NSFileProtectionComplete` key is loaded from the user keybag and unwrapped. It is a binary plist stored in the No Protection class, whose contents are encrypted with a key held in Effaceable Storage. In order to give forward security to keybags, this key is wiped and regenerated each time a user changes their passcode. The `AppleKeyStore` kernel extension manages the user keybag, and can be queried regarding a device's lock state. It reports that the device is unlocked only if all the class keys in the user keybag are accessible,
and have been unwrapped successfully.

Device keybag is used to store the wrapped class keys used for operations involving device-specific data. iOS devices configured for shared use sometimes need access to credentials before any user has logged in; therefore, a keybag that isn't protected by the user's passcode is required. iOS doesn't support cryptographic separation of per-user file system content, which means the system will use class keys from the device keybag to wrap per-file keys. The Keychain, however, uses class keys from the user keybag to protect items in the user Keychain. On iOS

devices configured for use by a single user (the default configuration), the device keybag and the user keybag are one and the same, and are protected by the user's passcode.

Backup keybag is created when an encrypted backup is made by iTunes and stored on the computer to which the device is backed up. A new keybag is created with a new set of keys, and the backed-up data is re-encrypted to these new keys. As explained previously, non-migratory Keychain items remain wrapped with the UID-derived key, allowing them to be restored to the device they were originally backed up from, but rendering them inaccessible on a different device.

The keybag is protected with the password set in iTunes, run through 10 million iterations of PBKDF2. Despite this large iteration count, there's no tie to a specific device, and therefore a brute-force attack parallelized across many computers could theoretically be attempted on the backup keybag. This threat can be mitigated with a sufficiently strong password.

If a user chooses not to encrypt an iTunes backup, the backup files aren't encrypted regardless of their Data Protection class, but the Keychain remains protected with a UID-derived key. This is why Keychain items migrate to a new device only if a backup password is set.

Escrow keybag is used for iTunes syncing and MDM. This keybag allows iTunes to back up and sync without requiring the user to enter a passcode, and it allows an MDM solution to remotely clear a user's passcode. It is stored on the computer that's used to sync with iTunes, or on the MDM solution that manages the device.

The escrow keybag improves the user experience during device synchronization, which potentially requires access to all classes of data. When a passcode-locked device is first connected to iTunes, the user is prompted to enter a passcode. The device then creates an escrow keybag containing the same class keys used on the device, protected by a newly generated key. The escrow keybag and the key protecting it are split between the device and the host or server, with the data stored on the device in the Protected Until First User Authentication class. This is why the device passcode must be entered before the user backs up with iTunes for the first time after a reboot.

In the case of an OTA software update, the user is prompted for their passcode when initiating the update. This is used to securely create a one-time Unlock Token, which unlocks the user keybag after the update. This token can't be generated without entering the user's passcode, and any previously generated token is invalidated if the user's passcode changed.

One-time Unlock Tokens are either for attended or unattended installation of a software update. They are encrypted with a key derived from the current value of a monotonic counter in the Secure Enclave, the UUID of the keybag, and the Secure Enclave's UID.

Incrementing the one-time Unlock Token counter in the Secure Enclave invalidates any existing token. The counter is incremented when a token is used, after the first unlock of a restarted device, when a software update is canceled (by the user or by the system), or when the policy timer for a token has expired.

The one-time Unlock Token for attended software updates expires after 20 minutes. This token is exported from the Secure Enclave and is written to Effaceable Storage. A policy timer increments the counter if the device hasn't rebooted within 20 minutes.

For an unattended software update, which is set when the user chooses "Install Later" when notified of the update, the application processor can keep the one-time Unlock Token alive in the Secure Enclave for up to 8 hours. After that time, a policy timer increments the counter.

iCloud Backup keybag is similar to the backup keybag. All the class keys in this keybag are asymmetric (using Curve25519, like the Protected Unless Open Data Protection class), so iCloud backups can be performed in the background. For all Data Protection classes except No Protection, the encrypted data is read from the device and sent to iCloud. The corresponding class keys are protected by iCloud keys. The Keychain class keys are wrapped with a UID-derived key in the same way as an unencrypted iTunes backup. An asymmetric keybag is also used for the backup in the Keychain recovery aspect of iCloud Keychain.

Security Certifications and programs

Note: For the latest information on iOS Security Certifications, validations, and guidance, go to: https://support.apple.com/kb/HT202739.

ISO 27001 and 27018 certifications

Apple has received ISO 27001 and ISO 27018 certification for the Information Security Management System for the infrastructure, development, and operations supporting these products and services: Apple School Manager, iCloud, iMessage, FaceTime, Managed Apple IDs, and iTunes U, in accordance with the Statement of Applicability v2.1 dated July 11, 2017. Apple's compliance with the ISO standard was certified by the British Standards Institution. The BSI website has certificates of compliance for ISO 27001 and ISO 27018. To view these certificates, go to:

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Cryptographic validation (FIPS 140-2)

The cryptographic modules in iOS have been repeatedly validated for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 following each release since iOS 6. As with each major release, Apple submits the modules to CMVP for re-validation when the iOS operating system is released. This program validates the integrity of cryptographic operations for Apple apps and third-party apps that properly utilize iOS cryptographic services and approved algorithms.

Common Criteria Certification (ISO 15408)

Since the release of iOS 9, Apple has achieved iOS certifications for each major iOS release under the Common Criteria Certification program for the following:

- Mobile Device Fundamental Protection Profile
- VPN IPSec Client Protection Profile
- Extended Package for Mobile Device Management Agents
- Extended Package for Wireless LAN Clients

iOS 11 is expected to include additional certifications for the following:

- Application Software Protection Profile
- Extended Package for Email Clients
- Extended Package for Web Browsers

Apple plans to do so with each successive major release of iOS. Apple has taken an active role within the International Technical Community (ITC) in developing currently unavailable Collaborative Protection Profiles (cPPs) focused on evaluating key mobile security technology. Apple continues to evaluate and pursue certifications against new and updated versions of the cPPs available today.

Commercial Solutions for Classified (CSfC)

Where applicable, Apple has also submitted the iOS platform and various services for inclusion in the Commercial Solutions for Classified (CSfC) Program Components List. As Apple platforms and services undergo Common Criteria Certifications, they will be submitted for inclusion under CSfC Program Components List as well.

To view the most recently listed components, go to: https://www.nsa.gov/resources/everyone/csfc/components-list/

Security configuration guides

Apple has collaborated with governments worldwide to develop guides that give instructions and recommendations for maintaining a more secure environment, also known as device hardening for high-risk environments. These guides provide defined and vetted information about how to configure and utilize built-in features in iOS for enhanced protection.

App Security

Apps are among the most critical elements of a modern mobile security architecture. While apps provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

Because of this, iOS provides layers of protection to ensure that apps are signed and verified, and are sandboxed to protect user data. These elements provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps on iOS without impacting system integrity. And users can access these apps on their iOS devices without undue fear of viruses, malware, or unauthorized attacks.

App code signing

Once the iOS kernel has started, it controls which user processes and apps can be run. To ensure that all apps come from a known and approved source and haven't been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate. Apps provided with the device, like Mail and Safari, are signed by Apple. Third-party apps must also be validated and signed using an Apple-issued certificate. Mandatory code signing extends the concept of chain of trust from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code.

In order to develop and install apps on iOS devices, developers must register with Apple and join the Apple Developer Program. The real-world identity of each developer, whether an individual or a business, is verified by Apple before their certificate is issued. This certificate enables developers to sign apps and submit them to the App Store for distribution. As a result, all apps in the App Store have been submitted by an identifiable person or organization, serving as a deterrent to the creation of malicious apps. They have also been reviewed by Apple to ensure they operate as described and don't contain obvious bugs or other problems. In addition to the technology already discussed, this curation process gives customers confidence in the quality of the apps they buy.

iOS allows developers to embed frameworks inside of their apps, which can be used by the app itself or by extensions embedded within the app. To protect the system and other apps from loading third-party code inside of their address space, the system will perform a code signature validation of all the dynamic libraries that a process links against at launch time. This verification is accomplished through the team identifier (Team ID), which is extracted from an Apple-issued certificate. A team identifier is a 10-character alphanumeric string; for example, 1A2B3C4D5F. A program may link against any platform library that ships with the system or any library with the same team identifier in its code signature as the main executable. Since the executables shipping as part of the system don't have a team identifier, they can only link against libraries that ship with the system itself.

Businesses also have the ability to write in-house apps for use within their organization and distribute them to their employees. Businesses and organizations can apply to the Apple Developer Enterprise Program (ADEP) with a D-U-N-S number. Apple approves applicants after verifying their identity and eligibility. Once an organization becomes a member of ADEP, it can register to obtain a Provisioning Profile that permits in-house apps to run on devices it authorizes. Users must have the Provisioning Profile installed to run the in-house apps. This ensures that only the organization's intended users are able to load the apps onto their iOS devices. Apps installed via MDM are implicitly trusted because the relationship between the organization and the device is already established. Otherwise, users have to approve the app's Provisioning Profile in Settings. Organizations can restrict users from approving apps from unknown developers. On first launch of any enterprise app, the device must receive positive confirmation from Apple that the app is allowed to run.

Unlike other mobile platforms, iOS doesn't allow users to install potentially malicious unsigned apps from websites, or run untrusted code. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app hasn't been modified since it was installed or last updated.

Runtime process security

Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system.

All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS.

System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted as read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs don't allow apps to escalate their own privileges to modify other apps or iOS itself.

Access by third-party apps to user information and features such as iCloud and extensibility is controlled using declared entitlements. Entitlements are key value pairs that are signed in to an app and allow authentication beyond runtime factors, like UNIX user ID. Since entitlements are digitally signed, they can't be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system app or daemon.

In addition, apps can only perform background processing through system-provided APIs. This enables apps to continue to function without degrading performance or dramatically impacting battery life.

Address space layout randomization (ASLR) protects against the exploitation of memory corruption bugs. Built-in apps use ASLR to ensure that all memory regions are randomized upon launch. Randomly arranging the memory addresses of executable code, system libraries, and related programming constructs reduces the likelihood of many sophisticated exploits. For example, a return-to-libc attack attempts to trick a device into executing malicious code by manipulating memory addresses of the stack and system libraries. Randomizing the placement of these makes the attack far more difficult to execute, especially across multiple devices. Xcode, the iOS development environment, automatically compiles third-party programs with ASLR support turned on.

Further protection is provided by iOS using ARM's Execute Never (XN) feature, which marks memory pages as non-executable. Memory pages marked as both writable and executable can be used only by apps under tightly controlled conditions: The kernel checks for the presence of the Apple-only dynamic code-signing entitlement. Even then, only a single mmap call can be made to request an executable and writable page, which is given a randomized address. Safari uses this functionality for its JavaScript JIT compiler.

Extensions

iOS allows apps to provide functionality to other apps by providing *extensions*. Extensions are special-purpose signed executable binaries, packaged within an app. The system automatically detects extensions at install time and makes them available to other apps using a matching system.

A system area that supports extensions is called an *extension point*. Each extension point provides APIs and enforces policies for that area. The system determines which extensions are available based on extension point–specific matching rules. The system automatically launches extension processes as needed and manages their lifetime. Entitlements can be used to restrict extension availability to particular system apps. For example, a Today view widget appears only in Notification Center, and a sharing extension is available only from the Sharing pane. The extension points are Today widgets, Share, Custom actions, Photo Editing, Document Provider, and Custom Keyboard.

Extensions run in their own address space. Communication between the extension and the app from which it was activated uses interprocess communications mediated by the system framework. They don't have access to each other's files or memory spaces. Extensions are designed to be isolated from each other, from their containing apps, and from the apps that use them. They are sandboxed like any other third-party app and have a container separate from the containing app's container. However, they share the same access to privacy controls as the container app. So if a user grants Contacts access to an app, this grant will be extended to the extensions that are embedded within the app, but not to the extensions activated by the app.

Custom keyboards are a special type of extension since they're enabled by the user for the entire system. Once enabled, a keyboard extension is used for any text field except the passcode input and any secure text view. To restrict the transfer of user data, custom keyboards run by default in a very restrictive sandbox that blocks access to the network, to services that perform network operations on behalf of a process,

and to APIs that would allow the extension to exfiltrate typing data. Developers of custom keyboards can request that their extension have Open Access, which will let the system run the extension in the default sandbox after getting consent from the user.

For devices enrolled in an MDM solution, document and keyboard extensions obey Managed Open In rules. For example, the MDM solution can prevent a user from exporting a document from a managed app to an unmanaged Document Provider, or using an unmanaged keyboard with a managed app. Additionally, app developers can prevent the use of third-party keyboard extensions within their app.

App Groups

Apps and extensions owned by a given developer account can share content when configured to be part of an App Group. It is up to the developer to create the appropriate groups on the Apple Developer Portal and include the desired set of apps and extensions. Once configured to be part of an App Group, apps have access to the following:

- A shared on-volume container for storage, which stays on the device as long as at least one app from the group is installed
- Shared preferences
- Shared Keychain items

The Apple Developer Portal guarantees that App Group IDs are unique across the app ecosystem.

Data Protection in apps

The iOS Software Development Kit (SDK) offers a full suite of APIs that make it easy for third-party and in-house developers to adopt Data Protection and help ensure the highest level of protection in their apps. Data Protection is available for file and database APIs, including NSFileManager, CoreData, NSData, and SQLite.

The Mail app database (including attachments), managed books, Safari bookmarks, app launch images, and location data are also stored encrypted with keys protected by the user's passcode on their device. Calendar (excluding attachments), Contacts, Reminders, Notes, Messages, and Photos implement Protected Until First User Authentication.

User-installed apps that don't opt-in to a specific Data Protection class receive Protected Until First User Authentication by default.

Accessories

The Made for iPhone, iPad, and iPod touch (MFi) licensing program provides vetted accessory manufacturers access to the iPod Accessories Protocol (iAP) and the necessary supporting hardware components.

When an MFi accessory communicates with an iOS device using a Lightning connector or via Bluetooth, the device asks the accessory to prove it has been authorized by Apple by responding with an Apple-provided certificate, which is verified by the device. The device then sends a challenge, which the accessory must answer with a signed

response. This process is entirely handled by a custom integrated circuit (IC) that Apple provides to approved accessory manufacturers and is transparent to the accessory itself.

Accessories can request access to different transport methods and functionality; for example, access to digital audio streams over the Lightning cable, or location information provided over Bluetooth. An authentication IC ensures that only approved accessories are granted full access to the device. If an accessory doesn't support authentication, its access is limited to analog audio and a small subset of serial (UART) audio playback controls.

AirPlay also utilizes the authentication IC to verify that receivers have been approved by Apple. AirPlay audio and CarPlay video streams utilize the MFi-SAP (Secure Association Protocol), which encrypts communication between the accessory and device using AES-128 in CTR mode. Ephemeral keys are exchanged using ECDH key exchange (Curve25519) and signed using the authentication IC's 1024-bit RSA key as part of the Station-to-Station (STS) protocol.

HomeKit

HomeKit provides a home automation infrastructure that utilizes iCloud and iOS security to protect and synchronize private data without exposing it to Apple.

HomeKit identity

HomeKit identity and security are based on Ed25519 public-private key pairs. An Ed25519 key pair is generated on the iOS device for each user for HomeKit, which becomes their HomeKit identity. It is used to authenticate communication between iOS devices, and between iOS devices and accessories.

The keys are stored in Keychain and are included only in encrypted Keychain backups. The keys are synchronized between devices using iCloud Keychain.

Communication with HomeKit accessories

HomeKit accessories generate their own Ed25519 key pair for use in communicating with iOS devices. If the accessory is restored to factory settings, a new key pair is generated.

To establish a relationship between an iOS device and a HomeKit accessory, keys are exchanged using Secure Remote Password (3072-bit) protocol utilizing an eight-digit code provided by the accessory's manufacturer, entered on the iOS device by the user, and then encrypted using ChaCha20-Poly1305 AEAD with HKDF-SHA-512 derived keys. The accessory's MFi certification is also verified during setup.

When the iOS device and the HomeKit accessory communicate during use, each authenticates the other utilizing the keys exchanged in the above process. Each session is established using the Station-to-Station protocol and is encrypted with HKDF-SHA-512 derived keys based on per-session Curve25519 keys. This applies to both IP-based and Bluetooth Low Energy accessories.

Local data storage

HomeKit stores data about the homes, accessories, scenes, and users on a user's iOS device. This stored data is encrypted using keys derived from the user's HomeKit identity keys, plus a random nonce. Additionally, HomeKit data is stored using Data Protection class Protected Until First User Authentication. HomeKit data is only backed up in encrypted backups, so, for example, unencrypted iTunes backups don't contain HomeKit data.

Data synchronization between devices and users

HomeKit data can be synchronized between a user's iOS devices using iCloud and iCloud Keychain. The HomeKit data is encrypted during the synchronization using keys derived from the user's HomeKit identity and random nonce. This data is handled as an opaque blob during synchronization. The most recent blob is stored in iCloud to enable synchronization, but it isn't used for any other purposes. Because it is encrypted using keys that are available only on the user's iOS devices, its contents are inaccessible during transmission and iCloud storage.

HomeKit data is also synchronized between multiple users of the same home. This process uses authentication and encryption that is the same as that used between an iOS device and a HomeKit accessory. The authentication is based on Ed25519 public keys that are exchanged between the devices when a user is added to a home. After a new user is added to a home, all further communication is authenticated and encrypted using Station-to-Station protocol and per-session keys.

The user who initially created the home in HomeKit or another user with editing permissions can add new users. The owner's device configures the accessories with the public key of the new user so that the accessory can authenticate and accept commands from the new user. When a user with editing permissions adds a new user, the process is delegated to a home hub to complete the operation.

The process to provision Apple TV for use with HomeKit is performed automatically when the user signs in to iCloud. The iCloud account needs to have two-factor authentication enabled. Apple TV and the owner's device exchange temporary Ed25519 public keys over iCloud. When the owner's device and Apple TV are on the same local network, the temporary keys are used to secure a connection over the local network using Station-to-Station protocol and per-session keys. This process uses authentication and encryption that is the same as that used between an iOS device and a HomeKit accessory. Over this secure local connection, the owner's device transfers the user's Ed25519 public-private key pairs to Apple TV. These keys are then used to secure the communication between Apple TV and the HomeKit accessories and also between Apple TV and other iOS devices that are part of the HomeKit home.

If a user doesn't have multiple devices, and refuses to grant additional users access to their home, no HomeKit data is synchronized to iCloud.

Home data and apps

Access to home data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request home data, similar to Contacts, Photos, and other iOS data sources. If the user approves, apps have access to the names of rooms, names of accessories, and which room each accessory is in, and other information as detailed in the HomeKit developer documentation at: https://developer.apple.com/homekit/.

HomeKit and Siri

Siri can be used to query and control accessories, and to activate scenes. Minimal information about the configuration of the home is provided anonymously to Siri, to provide names of rooms, accessories, and scenes that are necessary for command recognition. Audio sent to Siri may denote specific accessories or commands, but such Siri data isn't associated with other Apple features such as HomeKit. For more information, refer to "Siri" in the Internet Services section of this paper.

HomeKit IP cameras

IP cameras in HomeKit send video and audio streams directly to the iOS device on the local network accessing the stream. The streams are encrypted using randomly generated keys on the iOS device and the IP camera, which are exchanged over the secure HomeKit session to the camera. When the iOS device isn't on the local network, the encrypted streams are relayed via the home hub to the iOS device. The home hub doesn't decrypt the streams and only functions as a relay between the iOS device and the IP camera. When an app displays the HomeKit IP camera video view to the user, HomeKit is rendering the video frames securely from a separate system process so the app is unable to access or store the video stream. In addition, apps are not permitted to capture screenshots from this stream.

iCloud remote access for HomeKit accessories

HomeKit accessories can connect directly with iCloud to enable iOS devices to control the accessory when Bluetooth or Wi-Fi communication isn't available.

iCloud remote access has been carefully designed so that accessories can be controlled and send notifications without revealing to Apple what the accessories are, or what commands and notifications are being sent. HomeKit doesn't send information about the home over iCloud remote access.

When a user sends a command using iCloud remote access, the accessory and iOS device are mutually authenticated and data is encrypted using the same procedure described for local connections. The contents of the communications are encrypted and not visible to Apple. The addressing through iCloud is based on the iCloud identifiers registered during the setup process.

Accessories that support iCloud remote access are provisioned during the accessory's setup process. The provisioning process begins with the user signing in to iCloud. Next, the iOS device asks the accessory to sign a challenge using the Apple Authentication Coprocessor that's built into all Built for HomeKit accessories. The accessory also generates prime256v1 elliptic curve keys, and the public key is sent to the

iOS device along with the signed challenge and the X.509 certificate of the authentication coprocessor. These are used to request a certificate for the accessory from the iCloud provisioning server. The certificate is stored by the accessory, but it doesn't contain any identifying information about the accessory, other than it has been granted access to HomeKit iCloud remote access. The iOS device that is conducting the provisioning also sends a bag to the accessory, which contains the URLs and other information needed to connect to the iCloud remote access server. This information isn't specific to any user or accessory.

Each accessory registers a list of allowed users with the iCloud remote access server. These users have been granted the ability to control the accessory by the person who added the accessory to the home. Users are granted an identifier by the iCloud server and can be mapped to an iCloud account for the purpose of delivering notification messages and responses from the accessories. Similarly, accessories have iCloud-issued identifiers, but these identifiers are opaque and don't reveal any information about the accessory itself.

When an accessory connects to the HomeKit iCloud remote access server, it presents its certificate and a pass. The pass is obtained from a different iCloud server and it isn't unique for each accessory. When an accessory requests a pass, it includes its manufacturer, model, and firmware version in its request. No user-identifying or home-identifying information is sent in this request. The connection to the pass server isn't authenticated, in order to help protect privacy.

Accessories connect to the iCloud remote access server using HTTP/2, secured using TLS v1.2 with AES-128-GCM and SHA-256. The accessory keeps its connection to the iCloud remote access server open so that it can receive incoming messages and send responses and outgoing notifications to iOS devices.

SiriKit

Siri utilizes the iOS Extension mechanism to communicate with third-party apps. Although Siri has access to iOS contacts and the device's current location, Siri checks the permission to access iOS-protected user data of the app containing the Extension to see if the app has access before providing that information to it. Siri passes only the relevant fragment of the original user query text to the extension. For example, if the app doesn't have access to iOS contacts, Siri won't resolve a relationship in a user request such as "Pay my mother 10 dollars using PaymentApp." In this case, the Extension's app would only see "mother" through the raw utterance fragment being passed to it. However, if the app does have iOS contacts access, it would receive the iOS contact information for the user's mother. If a contact were referred to in the body of a message—for example, "Tell my mother on Message app that my brother is awesome"—Siri wouldn't resolve "my brother" regardless of the app's TCCs. Content presented by the app may be sent to the server to allow Siri to understand vocabulary a user may use in the app.

In cases like "Get me a ride to my mom's home using <app name>"—where the user's request requires location information to be retrieved from the user's contacts, Siri provides that location information to the app's extension, for that request only, regardless of the app's location or contacts access.

At runtime, Siri allows the SiriKit-enabled app to provide a set of custom words specific to application instance. These custom words are tied to the random identifier discussed in the Siri section of this paper, and have the same lifetime.

HealthKit

HealthKit stores and aggregates data from health and fitness apps with permission of the user. HealthKit also works directly with health and fitness devices, such as compatible Bluetooth LE heart rate monitors and the motion coprocessor built into many iOS devices.

Health data

HealthKit stores and aggregates the user's health data, such as height, weight, distance walked, blood pressure, and so on. This data is stored in Data Protection class Complete Protection, which means it is accessible only after a user enters their passcode or uses Touch ID or Face ID to unlock the device.

HealthKit also aggregates management data, such as access permissions for apps, names of devices connected to HealthKit, and scheduling information used to launch apps when new data is available. This data is stored in Data Protection class Protected Until First User Authentication.

Temporary journal files store health records that are generated when the device is locked, such as when the user is exercising. These are stored in Data Protection class Protected Unless Open. When the device is unlocked, the temporary journal files are imported into the primary health databases, then deleted when the merge is completed.

Health data can be stored in iCloud. When configured for iCloud storage, Health data is synced between devices and secured by encryption that protects the data both in transit and at rest. Health data is only included in encrypted iTunes Backups. It is not included in either unencrypted iTunes backups or iCloud Backup.

Data integrity

Data stored in the database includes metadata to track the provenance of each data record. This metadata includes an app identifier that identifies which app stored the record. Additionally, an optional metadata item can contain a digitally signed copy of the record. This is intended to provide data integrity for records generated by a trusted device. The format used for the digital signature is the Cryptographic Message Syntax (CMS) specified in IETF RFC 5652.

Access by third-party apps

Access to the HealthKit API is controlled with entitlements, and apps must conform to restrictions about how the data is used. For example, apps aren't allowed to utilize health data for advertising. Apps are also required to provide users with a privacy policy that details its use of health data.

Access to health data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request access to health data, similar to Contacts, Photos, and other iOS data sources. However, with health data, apps are granted separate access for reading and writing data, as well as separate access for each type of health data. Users can view, and revoke, permissions they've granted for accessing health data in the Sources tab of the Health app.

If granted permission to write data, apps can also read the data they write. If granted the permission to read data, they can read data written by all sources. However, apps can't determine access granted to other apps. In addition, apps can't conclusively tell if they have been granted read access to health data. When an app doesn't have read access, all queries return no data—the same response as an empty database would return. This prevents apps from inferring the user's health status by learning which types of data the user is tracking.

Medical ID

The Health app gives users the option of filling out a Medical ID form with information that could be important during a medical emergency. The information is entered or updated manually and isn't synchronized with the information in the health databases.

The Medical ID information is viewed by tapping the Emergency button on the Lock screen. The information is stored on the device using Data Protection class No Protection so that it is accessible without having to enter the device passcode. Medical ID is an optional feature that enables users to decide how to balance both safety and privacy concerns.

ReplayKit

ReplayKit is a framework that allows developers to add recording and live broadcasting capabilities to their apps. In addition, it allows users to annotate their recordings and broadcasts using the device's front-facing camera and microphone.

Movie recording

There are several layers of security built into recording a movie:

- **Permissions dialog:** Before recording starts, ReplayKit presents a user consent alert requesting that the user acknowledge their intent to record the screen, the microphone, and the front-facing camera. This alert is presented once per app process, and will be re-presented if the app is left in the background for longer than 8 minutes.
- **Screen and audio capture:** Screen and audio capture occurs out of the app's process in ReplayKit's daemon *replayd*. This ensures the recorded content is never accessible to the app process.
- **Movie creation and storage:** The movie file is written to a directory that's only accessible to ReplayKit's subsystems and is never accessible to any apps. This prevents recordings being used by third parties without the user's consent.
- **End-user preview and sharing:** The user has the ability to preview and share the movie with UI vended by ReplayKit. The UI is presented out-of-process via the iOS Extension infrastructure and has access to the generated movie file.

Broadcasting

- **Screen and audio capture:** The screen and audio capture mechanism during broadcasting is identical to movie recording and occurs in *replayd*.
- **Broadcast extensions:** For third-party services to participate in ReplayKit broadcasting, they're required to create two new extensions that are configured with the com.apple.broadcast-services endpoint:
  - A UI extension that allows the user to set up their broadcast
  - An upload extension that handles uploading video and audio data to the service's back-end servers

The architecture ensures that hosting apps have no privileges to the broadcasted video and audio contents–only ReplayKit and the third-party broadcast extensions have access.

- **Broadcast picker:** To select which broadcast service to use, ReplayKit provides a view controller (similar to UIActivityViewController) that the developer can present in their app. The view controller is implemented using the UIRemoteViewController SPI and is an extension that lives within the ReplayKit framework. It is out-of-process from the hosting app.
- **Upload extension:** The upload extension that third-party broadcast services implement to handle video and audio content during broadcasting can choose to receive content in two ways:
  - Small encoded MP4 clips
  - Raw unencoded sample buffers
    - **MP4 clip handling:** During this mode of handling, the small encoded MP4 clips are generated by *replayd* and stored in a private location only accessible to ReplayKit's subsystems. Once a movie clip is generated, *replayd* will pass the location of the movie clip to the third-party upload extension via the NSExtension request SPI (XPC based). *replayd* also generates a one-time sandbox token that's also passed to the upload extension, which grants the extension access to the particular movie clip during the extension request.
    - **Sample buffer handling:** During this mode of handling, video and audio data is serialized and passed to the third-party upload extension in real time through a direct XPC connection. Video data is encoded by extracting the IOSurface object from the video sample buffer, encoding it securely as an XPC object, sending over via XPC to the third-party extension, and decoding securely back into an IOSurface object.

Secure Notes

The Notes app includes a Secure Notes feature that allows users to protect the contents of specific notes. Secure notes are encrypted using a user-provided passphrase that is required to view the notes on iOS, macOS, and the iCloud website.

When a user secures a note, a 16-byte key is derived from the user's passphrase using PBKDF2 and SHA256. The note's contents are encrypted using AES-GCM. New records are created in Core Data and CloudKit to store the encrypted note, tag, and initialization vector, and the original note records are deleted; the encrypted data isn't written in place. Attachments are also encrypted in the same way. Supported attachments include images, sketches, tables, maps, and websites. Notes containing other types of attachments can't be encrypted, and unsupported attachments can't be added to secure notes.

When a user successfully enters the passphrase, whether to view or create a secure note, Notes opens a secure session. While open, the user isn't required to enter the passphrase—or use Touch ID or Face ID—to view or secure other notes. However, if some notes have a different passphrase, the secure session applies only to notes protected with the current passphrase. The secure session is closed when:

- The user taps the Lock Now button in Notes.
- Notes is switched to the background for more than 3 minutes.
- The device locks.

Users who forget their passphrase can still view secure notes or secure additional notes if they enabled Touch ID or Face ID on their devices. In addition, Notes will show a user-supplied hint after three failed attempts to enter the passphrase. The user must know the current passphrase in order to change it.

Users can reset the passphrase if they have forgotten the current one. This feature allows users to create new secure notes with a new passphrase, but it won't allow them to see previously secured notes. The previously secured notes can still be viewed if the old passphrase is remembered. Resetting the passphrase requires the user's iCloud account passphrase.

Shared notes

Notes can be shared with others. Shared Notes are not end-to-end encrypted. Apple uses the CloudKit encrypted data type for any text or attachments that the user puts in a note. Assets are always encrypted with a key that's encrypted in the CKRecord. Metadata, such as the creation and modification dates, aren't encrypted. CloudKit manages the process by which participants can encrypt/decrypt each other's data.

Apple Watch

Apple Watch uses the security features and technology built for iOS to help protect data on the device, as well as communications with its paired iPhone and the Internet. This includes technologies such as Data Protection and Keychain access control. The user's passcode is also entangled with the device UID to create encryption keys.

Pairing Apple Watch with iPhone is secured using an out-of-band (OOB) process to exchange public keys, followed by the BTLE link shared secret. Apple Watch displays an animated pattern, which is captured by the camera on iPhone. The pattern contains an encoded secret that is used for BTLE 4.1 out-of-band pairing. Standard BTLE Passkey Entry is used as a fallback pairing method, if necessary.

Once the BTLE session is established, Apple Watch and iPhone exchange keys using a process adapted from IDS, as described in the iMessage section of this paper. Once keys have been exchanged, the Bluetooth session key is discarded, and all communications between Apple Watch and iPhone are encrypted using IDS, with the encrypted Bluetooth, Wi-Fi, and Cellular links providing a secondary encryption layer. Key rolling is utilized at 15-minute intervals to limit the exposure window, should traffic be compromised.

To support apps that need streaming data, encryption is provided using methods described under "FaceTime" in the Internet Services section of this paper, utilizing either the IDS service provided by the paired iPhone or a direct Internet connection.

Apple Watch implements hardware-encrypted storage and class-based protection of files and Keychain items, as described in the Encryption and Data Protection section of this paper. Access-controlled keybags for Keychain items are also used. Keys used for communications between the watch and iPhone are also secured using class-based protection.

When Apple Watch isn't within Bluetooth range, Wi-Fi or cellular can be used instead. Apple Watch won't join Wi-Fi networks unless the credentials—which must have previously been synced to Apple Watch—are already present on the paired iPhone. If Apple Watch is out of range of iPhone, any new network credentials on iPhone aren't on Apple Watch.

Apple Watch can be manually locked by holding down the side button. Additionally, motion heuristics are used to attempt to automatically lock the device shortly after it's removed from the wrist. When Apple Watch is locked, Apple Pay can only be used by entering the watch's passcode. Wrist detection is turned off using the Apple Watch app on iPhone. This setting can also be enforced using an MDM solution.

The paired iPhone can also unlock the watch, provided the watch is being worn. This is accomplished by establishing a connection authenticated by the keys established during pairing. iPhone sends the key, which the watch uses to unlock its Data Protection keys. The watch passcode isn't known to iPhone nor is it transmitted. This feature can be turned off using the Apple Watch app on iPhone.

Apple Watch can be paired with only one iPhone at a time. iPhone communicates instructions to erase all content and data from Apple Watch when unpaired.

Enabling Find My iPhone on the paired iPhone also allows the use of Activation Lock on Apple Watch. Activation Lock makes it harder for anyone to use or sell an Apple Watch that has been lost or stolen. Activation Lock requires the user's Apple ID and password to unpair, erase, or reactivate an Apple Watch.

Network Security

In addition to the built-in safeguards Apple uses to protect data stored on iOS devices, there are many network security measures that organizations can take to keep information secure as it travels to and from an iOS device.

Mobile users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they are authorized and their data is protected during transmission. iOS uses—and provides developer access to—standard networking protocols for authenticated, authorized, and encrypted communications. To accomplish these security objectives, iOS integrates proven technologies and the latest standards for both Wi-Fi and cellular data network connections.

On other platforms, firewall software is needed to protect open communication ports against intrusion. Because iOS achieves a reduced attack surface by limiting listening ports and removing unnecessary network utilities such as telnet, shells, or a web server, no additional firewall software is needed on iOS devices.

TLS

iOS supports Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) and DTLS. It supports both AES-128 and AES-256, and prefers cipher suites with perfect forward secrecy. Safari, Calendar, Mail, and other Internet apps automatically use this protocol to enable an encrypted communication channel between the device and network services. High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (SecureTransport) provide fine-grained control. CFNetwork disallows SSLv3, and apps that use WebKit (such as Safari) are prohibited from making an SSLv3 connection.

As of iOS 11 and macOS High Sierra, SHA-1 certificates are no longer allowed for TLS connections unless trusted by the user. Certificates with RSA keys shorter than 2048 bits are also disallowed. The RC4 symmetric cipher suite is deprecated in iOS 10 and macOS Sierra. By default, TLS clients or servers implemented with SecureTransport APIs don't have RC4 cipher suites enabled, and are unable to connect when RC4 is the only cipher suite available. To be more secure, services or apps that require RC4 should be upgraded to use modern, secure cipher suites.

App Transport Security

App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. By default, App Transport Security limits cipher selection to include only suites that provide forward secrecy, specifically ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode. Apps are able to disable the forward secrecy requirement per-domain, in which case RSA_AES is added to the set of available ciphers.

Servers must support TLS v1.2 and forward secrecy, and certificates must be valid and signed using SHA-256 or better with a minimum 2048-bit RSA key or 256-bit elliptic curve key.

Network connections that don't meet these requirements will fail, unless the app overrides App Transport Security. Invalid certificates always result in a hard failure and no connection. App Transport Security is automatically applied to apps that are compiled for iOS 9 or later.

VPN

Secure network services like virtual private networking typically require minimal setup and configuration to work with iOS devices. iOS devices work with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPSec with authentication by shared secret, RSA Certificates, ECDSA Certificates, EAP-MSCHAPv2, or EAP-TLS
- SSL-VPN using the appropriate client app from the App Store
- Cisco IPSec with user authentication by password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret and certificates
- L2TP/IPSec with user authentication by MS-CHAPV2 password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret

iOS supports the following:

- **VPN On Demand** for networks that use certificate-based authentication. IT policies specify which domains require a VPN connection by using a VPN configuration profile.
- **Per App VPN** for facilitating VPN connections on a much more granular basis. MDM can specify a connection for each managed app and specific domains in Safari. This helps ensure that secure data always goes to and from the corporate network—and that a user's personal data doesn't.
- **Always-on VPN,** which can be configured for devices managed via MDM and supervised using Apple Configurator 2, the Device Enrollment Program, or Apple School Manager. This eliminates the need for users to turn on VPN to enable protection when connecting to cellular and Wi-Fi networks. Always-on VPN gives an organization full control over device traffic by tunneling all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption. The organization can monitor and filter traffic to and from its devices, secure data within its network, and restrict device access to the Internet.

Wi-Fi

iOS supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data remains protected when sending and receiving communications over a Wi-Fi network connection. With support for 802.1X, iOS devices can be integrated into a broad range of RADIUS authentication environments.

802.1X wireless authentication methods supported on iPhone and iPad include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

Besides protection for data, iOS extends WPA2 level protection to unicast and multicast management frames through Protected Management Frame service referred in 802.11w. PMF support is available on iPhone 6 and iPad Air 2 or later.

iOS uses randomized Media Access Control (MAC) address when conducting Wi-Fi scans while it isn't associated with a Wi-Fi network. These scans could be performed in order to find and connect a preferred Wi-Fi network or to assist Location Services for apps that use geofences, such as location-based reminders or fixing a location in Apple Maps. Note that Wi-Fi scans which happen while trying to connect to a preferred Wi-Fi Network aren't randomized.

iOS also uses a randomized MAC address when conducting enhanced Preferred Network Offload (ePNO) scans when a device isn't associated with a Wi-Fi network or its processor is asleep. ePNO scans are run when a device uses Location Services for apps which use geofences, such as location-based reminders that determine whether the device is near a specific location.

Because a device's MAC address now changes when disconnected from a Wi-Fi network, it can't be used to persistently track a device by passive observers of Wi-Fi traffic, even when the device is connected to a cellular network. Apple has informed Wi-Fi manufacturers that iOS Wi-Fi scans use a randomized MAC address, and that neither Apple nor manufacturers can predict these randomized MAC addresses. Wi-Fi MAC address randomization support isn't available on iPhone4s or earlier.

On iPhone 6S or later, the hidden property of a known Wi-Fi network is known and updated automatically. If the Service Set Identifier (SSID) of a Wi-Fi network is broadcasted, the iOS device won't send a probe with the SSID included in the request. This prevents the device from broadcasting the network name of non-hidden networks.

To protect the device from vulnerabilities in network processor firmware, network interfaces including Wi-Fi and baseband have limited access to application processor memory. When USB or SDIO is used to interface with the network processor, the network processor cannot initiate Direct Memory Access (DMA) transactions to the application processor. When PCIe is used, each network processor is on its own isolated PCIe bus. An IOMMU on each PCIe bus limits the network processor's DMA access to pages of memory containing its network packets or control structures.

Bluetooth

Bluetooth support in iOS has been designed to provide useful functionality without unnecessary increased access to private data. iOS devices support Encryption Mode 3, Security Mode 4, and Service Level 1 connections. iOS supports the following Bluetooth profiles:

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Message Access Profile (MAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network Profile (PAN)
- Human Interface Device Profile (HID)
- Support for these profiles varies by device.

For more information, go to: https://support.apple.com/kb/ht3647.

Single Sign-on

iOS supports authentication to enterprise networks through Single Sign-on (SSO). SSO works with Kerberos-based networks to authenticate users to services they are authorized to access. SSO can be used for a range of network activities, from secure Safari sessions to third-party apps. Certificate-based authentication (PKINIT) is also supported.

iOS SSO utilizes SPNEGO tokens and the HTTP Negotiate protocol to work with Kerberos-based authentication gateways and Windows Integrated Authentication systems that support Kerberos tickets. SSO support is based on the open source Heimdal project.

The following encryption types are supported:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari supports SSO, and third-party apps that use standard iOS networking APIs can also be configured to use it. To configure SSO, iOS supports a configuration profile payload that allows MDM solutions to push down the necessary settings. This includes setting the user principal name (that is, the Active Directory user account) and Kerberos realm settings, as well as configuring which apps and Safari web URLs should be allowed to use SSO.

AirDrop security

iOS devices that support AirDrop use Bluetooth Low Energy (BLE) and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices, including AirDrop-capable Mac computers running OS X 10.11 or later. The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi Access Point.

When a user enables AirDrop, a 2048-bit RSA identity is stored on the device. Additionally, an AirDrop identity hash is created based on the email addresses and phone numbers associated with the user's Apple ID.

When a user chooses AirDrop as the method for sharing an item, the device emits an AirDrop signal over Bluetooth Low Energy. Other devices that are awake, in close proximity, and have AirDrop turned on detect the signal and respond with a shortened version of their owner's identity hash.

AirDrop is set to share with Contacts Only by default. Users can also choose to use AirDrop to share with everyone, or turn off the feature entirely. In Contacts Only mode, the received identity hashes are compared with hashes of people in the initiator's Contacts app. If a match is found, the sending device creates a peer-to-peer Wi-Fi network and advertises an AirDrop connection using Bonjour. Using this connection, the receiving devices send their full identity hashes to the initiator. If the full hash still matches Contacts, the recipient's first name and photo (if present in Contacts) are displayed in the AirDrop share sheet.

When using AirDrop, the sending user selects who they want to share with. The sending device initiates an encrypted (TLS) connection with the receiving device, which exchanges their iCloud identity certificates. The identity in the certificates is verified against each user's Contacts app. Then the receiving user is asked to accept the incoming transfer from the identified person or device. If multiple recipients have been selected, this process is repeated for each destination.

In the Everyone mode, the same process is used but if a match in Contacts isn't found, the receiving devices are shown in the AirDrop send sheet with a silhouette with the device's name, as defined in Settings > General > About > Name.

Organizations can restrict the use of AirDrop for devices or apps being managed by using an MDM solution.

Wi-Fi password sharing

iOS devices that support Wi-Fi password sharing use a mechanism similar to AirDrop to send a Wi-Fi password from one device to another.

When a user selects a Wi-Fi network (requestor) and is prompted for the Wi-Fi password, the Apple device starts a Bluetooth Low Energy advertisement indicating that it wants the Wi-Fi password. Other Apple devices that are awake, in close proximity, and have the password for the selected Wi-Fi network connect using Bluetooth Low Energy to the requesting device.

The device that has the Wi-Fi password (grantor) requires the Contact information of the requestor, and the requestor must prove their identity using a similar mechanism to AirDrop. Once identify is proven, the grantor sends the requestor the 64 character PSK, which can also be used to join the network.

Organizations can restrict the use of Wi-Fi password sharing for devices or apps being managed by using an MDM solution.

Apple Pay

With Apple Pay, users can use supported iOS devices and Apple Watch to pay in an easy, secure, and private way in stores, apps, and on the web in Safari. It's simple for users, and it's built with integrated security in both hardware and software.

Apple Pay is also designed to protect the user's personal information. Apple Pay doesn't collect any transaction information that can be tied back to the user. Payment transactions are between the user, the merchant, and the card issuer.

Apple Pay components

Secure Element: The Secure Element is an industry-standard, certified chip running the Java Card platform, which is compliant with financial industry requirements for electronic payments.

NFC controller: The NFC controller handles Near Field Communication protocols and routes communication between the application processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.

Wallet: Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay. Users can view their cards and additional information about their card issuer, their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in Setup Assistant and Settings.

Secure Enclave: On iPhone, iPad, and Apple Watch, the Secure Enclave manages the authentication process and enables a payment transaction to proceed.

On Apple Watch, the device must be unlocked, and the user must double-click the side button. The double-click is detected and passed to the Secure Element or Secure Enclave where available, directly without going through the application processor.

Apple Pay servers: The Apple Pay servers manage the setup and provisioning of credit and debit cards in Wallet and the Device Account Numbers stored in the Secure Element. They communicate both with the device and with the payment network servers. The Apple Pay servers are also responsible for re-encrypting payment credentials for payments within apps.

How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

How Apple Pay uses the NFC controller

As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.

Once payment is authorized by the cardholder using Touch ID or passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless transactions are contained to the local NFC field and are never exposed to the application processor. In contrast, payment authorization details for payments within apps and on the web are routed to the application processor, but only after encryption by the Secure Element to the Apple Pay Server.

Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields, Check Card,* and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone. Provisioning a card for Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.There are three ways to provision a credit, debit, or prepaid card into Apple Pay:

- Adding a card manually to Apple Pay
- Adding credit or debit cards on file from an iTunes Store account to Apple Pay
- Adding cards from a card issuer's app

Adding a credit or debit card manually to Apple Pay

To add a card manually, including store cards, the name, credit card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the camera on the device. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. Once all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

Adding credit or debit cards from an iTunes Store account to Apple Pay

For a credit or debit card on file with iTunes, the user may be required to re-enter their Apple ID password. The card number is retrieved from iTunes and the Check Card process is initiated. If the card is eligible for Apple Pay, the device will download and display terms and conditions, then send along the term's ID and the card security code to the Link and Provision process. Additional verification may occur for iTunes account cards on file.

Adding credit or debit cards from a card issuer's app

When the app is registered for use with Apple Pay, keys are established for the app and the merchant's server. These keys are used to encrypt the card information that's sent to the merchant, which prevents the information from being read by the iOS device. The provisioning flow is similar to that used for manually added cards, described previously, except one-time passwords are used in lieu of the CVV.

Additional verification

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, customer service call, or a method in an approved third-party app to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which the user will need to enter into Wallet, Settings, or the Apple Watch app. For customer service or verification using an app, the issuer performs their own communication process.

Payment authorization

On devices that have a Secure Enclave, the Secure Element will allow a payment to be made only after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID, Face ID, or the device passcode. Touch ID or Face ID is the default method if available, but the passcode can be used at any time. A passcode is automatically offered after three unsuccessful attempts to match a fingerprint or two unsuccessful attempts to match a face; after five unsuccessful attempts, the passcode is required. A passcode is also required when Touch ID or Face ID is not configured or not enabled for Apple Pay. On Apple Watch, the device must be unlocked with passcode and the side button must be double-clicked for a payment to be made.

Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the application processor. Though not directly connected, the Secure Enclave and Secure Element can communicate securely using a shared pairing key that is provisioned during the manufacturing process. The encryption and authentication of the communication are based on AES, with cryptographic nonces used by both sides to protect against replay attacks. The pairing key is generated inside the Secure Enclave from its UID key and the Secure Element's unique identifier. The pairing key is then securely transferred from the Secure Enclave to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the Secure Element.

When the user authorizes a transaction, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (AR) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and persists while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element via the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.

Credit, debit, and prepaid cards added to the Secure Element can only be used if the Secure Element is presented with authorization using the same pairing key and AR value from when the card was added. This allows iOS to instruct the Secure Enclave to render cards unusable by marking its copy of the AR as invalid under the following scenarios:

- When the passcode is disabled.
- The user signs out of iCloud.
- The user selects Erase All Content and Settings.
- The device is restored from recovery mode.

With Apple Watch, cards are marked as invalid when:

- The watch's passcode is disabled.
- The watch is unpaired from iPhone.
- Wrist detection is turned off.

Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for transactions within apps.

Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet.
- Another random number generated by the terminal—in the case of an NFC transaction.

  or

- Another random number generated by the server—in the case of transactions within apps.

These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

Contactless payments with Apple Pay

If iPhone is on and detects an NFC field, it will present the user with the relevant credit, debit, prepaid card, or the default card, which is managed in Settings. The user can also go to the Wallet app and choose a credit or debit card, or when the device is locked, double-click the Home button.

Next, the user must authenticate using Touch ID, Face ID, or their passcode before payment information is transmitted. When Apple Watch is unlocked, double-clicking the side button activates the default card for payment. No payment information is sent without user authentication. Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full actual credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services.

Paying with Apple Pay within apps

Apple Pay can also be used to make payments within iOS apps and Apple Watch apps as of watchOS 3. When users pay within apps using Apple Pay, Apple receives encrypted transaction information and re-encrypts it with a developer-specific key before it's sent to the developer or merchant. Apple Pay retains anonymous transaction information such as approximate purchase amount. This information can't be tied back to the user and never includes what the user is buying.

When an app initiates an Apple Pay payment transaction, the Apple Pay Servers receive the encrypted transaction from the device prior to the merchant receiving it. The Apple Pay Servers then re-encrypt it with a merchant-specific key before relaying the transaction to the merchant.

When an app requests a payment, it calls an API to determine if the device supports Apple Pay and if the user has credit or debit cards that can make payments on a payment network accepted by the merchant. The app requests any pieces of information it needs to process and fulfill the transaction, such as the billing and shipping address, and contact information. The app then asks iOS to present the Apple Pay sheet, which requests information for the app, as well as other necessary information, such as the card to use.

At this time, the app is presented with city, state, and zip code information to calculate the final shipping cost. The full set of requested information isn't provided to the app until the user authorizes the payment with Touch ID, Face ID, or the device passcode. Once the payment is authorized, the information presented in the Apple Pay sheet will be transferred to the merchant.

When the user authorizes the payment, a call is made to the Apple Pay Servers to obtain a cryptographic nonce, which is similar to the value returned by the NFC terminal used for in-store transactions. The nonce, along with other transaction data, is passed to the Secure Element to generate a payment credential that will be encrypted with an Apple key. When the encrypted payment credential comes out of the Secure Element, it's passed to the Apple Pay Servers, which decrypt the credential, verify the nonce in the credential against the nonce sent by

the Secure Element, and re-encrypt the payment credential with the merchant key associated with the Merchant ID. It's then returned to the device, which hands it back to the app via the API. The app then passes it along to the merchant system for processing. The merchant can then decrypt the payment credential with its private key for processing. This, together with the signature from Apple's servers, allows the merchant to verify that the transaction was intended for this particular merchant.

The APIs require an entitlement that specifies the supported Merchant IDs. An app can also include additional data to send to the Secure Element to be signed, such as an order number or customer identity, ensuring the transaction can't be diverted to a different customer. This is accomplished by the app developer, who can specify applicationData on the PKPaymentRequest. A hash of this data is included in the encrypted payment data. The merchant is then responsible for verifying that their applicationData hash matches what's included in the payment data.

Paying with Apple Pay on the web or with Handoff

Apple Pay can be used to make payments on websites. In iOS 10 or later, Apple Pay transactions can be made on the web on iPhone and iPad. Also, in macOS Sierra or later, Apple Pay transactions can start on a Mac and be completed on an Apple Pay enabled iPhone or Apple Watch using the same iCloud account.

Apple Pay on the web requires all participating websites to register with Apple. The Apple servers perform domain name validation and issue a TLS client certificate. Websites supporting Apple Pay are required to serve their content over HTTPS. For each payment transaction, websites need to obtain a secure and unique merchant session with an Apple server using the Apple-issued TLS client certificate. Merchant session data is signed by Apple. Once a merchant session signature is verified, a website may query whether the user has an Apple Pay capable device and whether they have a credit, debit, or prepaid card activated on the device. No other details are shared. If the user doesn't want to share this information, they can disable Apple Pay queries in Safari privacy settings on iOS and macOS.

Once a merchant session is validated, all security and privacy measures are the same as when a user pays within an app.

In the case of Mac to iPhone or Apple Watch Handoff, Apple Pay uses the end-to-end encrypted IDS protocol to transmit payment-related information between the user's Mac and the authorizing device. IDS uses the user's device keys to perform encryption so no other device can decrypt this information, and the keys aren't available to Apple. Device discovery for Apple Pay Handoff contains the type and unique identifier of the user's credit cards along with some metadata. The device-specific account number of the user's card isn't shared and it continues to remain stored securely on the user's iPhone or Apple Watch. Apple also securely transfers the user's recently used contact, shipping, and billing addresses over iCloud Keychain.

Once the user authorizes payment using Touch ID, Face ID, or their passcode on iPhone or double-clicks the side button on Apple Watch, a payment token uniquely encrypted to each website's merchant certificate is securely transmitted from the user's iPhone or Apple Watch to their Mac, and then delivered to the merchant's website.

Only devices in proximity to each other may request and complete payment. Proximity is determined through Bluetooth Low Energy advertisements.

Rewards cards

In iOS 9 or later, Apple Pay supports the Value Added Service (VAS) protocol for transmitting merchant rewards cards to compatible NFC terminals. The VAS protocol can be implemented on merchant terminals and uses NFC to communicate with supported Apple devices. The VAS protocol works over a short distance and is used to provide complementary services, such as transmission of rewards card information, as part of an Apple Pay transaction.

The NFC terminal initiates receiving the card information by sending a request for a card. If the user has a card with the store's identifier, the user is asked to authorize its use. If the merchant supports encryption, the card information, a timestamp, and a single-use random ECDH P-256 key is used with the merchant's public key to derive an encryption key for the card data, which is sent to the terminal. If the merchant doesn't support encryption, the user is asked to re-present the device to the terminal before the rewards card information is sent.

Apple Pay Cash

As of iOS 11.2 and watchOS 4.2, Apple Pay can be used on an iPhone, iPad, or Apple Watch to send, receive, and request money from other users. When a user receives money, its added to an Apple Pay Cash account that can be accessed in Wallet or within Settings > Wallet & Apple Pay across any of the eligible devices the user has signed in with their Apple ID.

To use person to person payments and Apple Pay Cash a user must be signed into their iCloud account on an Apple Pay Cash compatible device, and have two-factor authentication set up on the iCloud account.

When you set up Apple Pay Cash, the same information as when you add a credit or debit card may be shared with our partner bank Green Dot Bank and with Apple Payments Inc., a wholly owned subsidiary created to protect your privacy by storing and processing information separately from the rest of Apple and in a way that the rest of Apple doesn't know. This information is only used for troubleshooting, fraud prevention, and regulatory purposes.

Money requests and transfers between users are initiated from within the Messages app or by asking Siri. When a user attempts to send money, iMessage will display the Apple Pay sheet. The Apple Pay Cash balance is always used first. If necessary, additional funds are drawn from a second credit or debit card the user has added to Wallet.

The Apple Pay Cash card in Wallet can be used with Apple Pay to make payments in stores, in apps, and on the web. Money in the Apple Pay Cash account can also be transferred to a bank account. In addition to receiving money from another user, money can be added to the Apple Pay Cash account from a debit or prepaid card in Wallet.

Apple Payments Inc. will store and may use your transaction data for troubleshooting, fraud prevention, and regulatory purposes once a transaction is completed. The rest of Apple doesn't know who you sent money to, received money from, or where you made a purchase with your Apple Pay Cash card.

When the user sends money with Apple Pay, adds money to an Apple Pay Cash account, or transfers money to a bank account, a call is made to the Apple Pay Servers to obtain a cryptographic nonce, which is similar to the value returned for Apple Pay within apps. The nonce, along with other transaction data, is passed to the Secure Element to generate a payment signature. When the payment signature comes out of the Secure Element, it's passed to the Apple Pay Servers. The authentication, integrity, and correctness of the transaction is verified via the payment signature and the nonce by Apple Pay Servers. Money transfer is then initiated and the user is notified of transaction completion.

If the transaction involves a credit or debit card for:

- Adding money to Apple Pay Cash or
- Sending money to another user or
- Providing supplemental money if the Apple Pay Cash balance is insufficient

Then, in addition to the transfer signature described above, an encrypted payment credential is also produced and sent to Apple Pay Servers—which is similar to what is used for Apple Pay within apps and websites.

Once the balance of the Apple Pay Cash account exceeds a certain amount, or if unusual activity is detected, the user will be prompted to verify their identity. Information provided to verify the user's identity, such as social security number or answers to questions (e.g., confirm street name you have previously lived on) is securely transmitted to Apple's partner and encrypted using their key. Apple cannot decrypt this data.

Suica cards

In Japan, users can add a Suica card to Apple Pay Wallet on supported models of iPhone and Apple Watch. This can be done either by transferring the value and commuter pass from a physical card into its digital Wallet representation or by provisioning a new Suica into Wallet from the Suica app. After Suica cards are added to Wallet, users can pay in stores or ride transit with their anonymous Suica card, MySuica card, or card that contains a commuter pass.

Added Suica cards are associated with a user's iCloud account. If the user adds more than one card to Wallet, Apple or the transit issuer may be able to link the user's personal information and the associated account information between cards. For example, MySuica cards can be linked to anonymous Suica cards. Suica cards and transactions are protected by a set of hierarchical cryptographic keys.

During the process of transferring the balance from physical card to Wallet, if the card is an anonymous Suica card, users are required to enter the last four digits of the card's serial number. If the card is a MySuica card or a card that contains a commuter pass, users must also enter their date of birth as proof of card possession. When transferring passes from iPhone to Apple Watch, both devices must be online during transfer.

The balance can be recharged with funds from credit and prepaid cards via Wallet or from the Suica app. The security of reloading the balance when using Apple Pay, is described in the "Paying with Apple Pay within apps" section of this paper.

The process of provisioning the Suica card from within the Suica app is described in the "Adding credit or debit cards from a card issuer's app" section of this paper.

The transit issuer has the cryptographic keys needed to authenticate to the physical card and verify user's entered data. Once verified, the system can create a Device Account Number for the Secure Element and activate the newly added pass in Wallet with the transferred balance. Once provisioning from plastic is complete, the physical card is disabled.

At the end of either type of provisioning, the Suica balance is encrypted and stored to a designated applet in the Secure Element. The transit operator has the keys to perform cryptographic operations on the card data for balance transactions.

By default, users benefit from the seamless Express Transit experience that allows them to pay and ride without requiring Touch ID, Face ID, or a passcode. Information like recently visited stations, transaction history, and additional tickets may be accessed by any nearby contactless card reader with Express Mode enabled. Users can enable the Touch ID, Face ID, or passcode authorization requirement in the Wallet & Apple Pay settings by disabling Express Transit.

As with other Apple Pay cards, users can suspend or remove Suica cards by:

- Erasing the device remotely with Find My iPhone
- Enabling Lost Mode with Find My iPhone
- MDM remote wipe operations
- Removing all cards from their Apple ID account page
- Removing all cards from iCloud.com
- Removing all cards from Wallet

Apple Pay Servers notify the transit operator to disable those Suica cards. If their device is offline when they try to erase it, their Suica cards might still be available for use at some terminals until 12:01 AM JST the following day.

If users remove their Suica cards, the balance is recoverable. They can add them back to a device signed in with the same Apple ID after 5:00 AM JST the following day.

Suica cards can't be suspended if your device is offline.

Suspending, removing, and erasing cards

Users can suspend Apple Pay on iPhone, iPad, and Apple Watch running watchOS 3 by placing their devices in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone, iCloud.com, or directly on their devices using Wallet. On Apple Watch, cards can be removed using iCloud settings, the Apple Watch app on iPhone, or directly on the watch. The ability to make payments using cards on the device will be suspended or removed from Apple Pay by the card issuer or respective payment network even if the device is offline and not connected to a cellular or Wi-Fi network. Users can also call their card issuer to suspend or remove cards from Apple Pay.

Additionally, when a user erases the entire device using "Erase All Content and Settings," using Find My iPhone, or restoring their device in recovery mode, iOS will instruct the Secure Element to mark all cards as deleted. This has the effect of immediately changing the cards to an unusable state until the Apple Pay Servers can be contacted to fully erase the cards from the Secure Element. Independently, the Secure Enclave marks the AR as invalid, so that further payment authorizations for previously enrolled cards aren't possible. When the device is online, it attempts to contact the Apple Pay Servers to ensure all cards in the Secure Element are erased.

Internet Services

Creating strong Apple ID passwords
Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:

- At least eight characters
- At least one letter
- At least one uppercase letter
- At least one number
- No more than three consecutive identical characters
- Not the same as the account name

Apple has built a robust set of services to help users get even more utility and productivity out of their devices, including iMessage, FaceTime, Siri Suggestions, iCloud, iCloud Backup, and iCloud Keychain.

These Internet services have been built with the same security goals that iOS promotes throughout the platform. These goals include secure handling of data, whether at rest on the device or in transit over wireless networks; protection of users' personal information; and threat protection against malicious or unauthorized access to information and services. Each service uses its own powerful security architecture without compromising the overall ease of use of iOS.

Apple ID

An Apple ID is the account that is used to sign in to Apple services such as iCloud, iMessage, FaceTime, the iTunes Store, the iBooks Store, the App Store, and more. It is important for users to keep their Apple IDs secure to prevent unauthorized access to their accounts. To help with this, Apple requires strong passwords that must be at least eight characters in length, contain both letters and numbers, must not contain more than three consecutive identical characters, and can't be a commonly used password. Users are encouraged to exceed these guidelines by adding extra characters and punctuation marks to make their passwords even stronger. Apple also requires users to set up three security questions that can be used to help verify the owner's identity when making changes to their account information or resetting a forgotten password.

Apple also sends email and push notifications to users when important changes are made to their account; for example, if a password or billing information has been changed, or the Apple ID has been used to sign in on a new device. If anything looks unfamiliar, users are instructed to change their Apple ID password immediately.

In addition, Apple employs a variety of policies and procedures designed to protect user accounts. These include limiting the number of retries for sign-in and password reset attempts, active fraud monitoring to help identify attacks as they occur, and regular policy reviews that allow Apple to adapt to any new information that could affect customer security.

Two-factor authentication

To help users further secure their accounts, Apple offers *two-factor authentication*—an extra layer of security for Apple IDs. It is designed to ensure that only the account's owner can access the account, even if someone else knows the password.

With two-factor authentication, a user's account can be accessed only on trusted devices, such as the user's iPhone, iPad, or Mac. To sign in for the first time on any new device, two pieces of information are required—the Apple ID password and a six-digit verification code that's automatically displayed on the user's trusted devices or sent to a trusted phone number. By entering the code, the user verifies that they trust the new device and

that it's safe to sign in. Because a password alone is no longer enough to access a user's account, two-factor authentication improves the security of the user's Apple ID and all the personal information they store with Apple. It is integrated directly into iOS, macOS, tvOS, watchOS, and the authentication systems used by Apple's websites.

For more information on two-factor authentication, go to: https://support.apple.com/HT204915.

Two-step verification

Since 2013, Apple has also offered a similar security method called *two-step verification*. With two-step verification enabled, the user's identity must be verified via a temporary code sent to one of the user's trusted devices before changes are permitted to their Apple ID account information; before signing in to iCloud, iMessage, FaceTime, or Game Center; and before making an iTunes Store, iBooks Store, or App Store purchase from a new device. Users are also provided with a 14-character Recovery Key to be stored in a safe place in case they ever forget their password or lose access to their trusted devices. While most new users will be encouraged to use two-factor authentication, there are still some situations where two-step verification is recommended instead.

For more information on two-step verification for Apple ID, go to: https://support.apple.com/kb/ht5570

Managed Apple IDs

Managed Apple IDs function in a way similar to an Apple ID, but are owned and controlled by an educational institution. The institution can reset passwords, limit purchasing and communications such as FaceTime and Messages, and set up role-based permissions for staff members, teachers, and students.

Some Apple services are disabled for Managed Apple IDs, such as Apple Pay, iCloud Keychain, HomeKit, and Find My iPhone.

For more information about Managed Apple IDs, go to: https://help.apple.com/schoolmanager/

Auditing Managed Apple IDs

Managed Apple IDs also support auditing, which allows institutions to comply with legal and privacy regulations. Administrator, manager, or teacher accounts can be granted auditing privileges for specific Managed Apple IDs. Auditors can monitor only accounts that are below them in the school's hierarchy. That is, teachers can monitor students; managers can audit teachers and students; and administrators can audit managers, teachers, and students.

When auditing credentials are requested using Apple School Manager, a special account is issued that has access only to the Managed Apple ID for which auditing was requested. Auditing permission expires after seven days. During that period, the auditor can read and modify the user's content stored in iCloud or CloudKit-enabled apps. Every request for auditing access is logged in Apple School Manager. The logs show who the auditor was, the Managed Apple ID the auditor requested access to, the time of the request, and if the auditing was performed.

Managed Apple IDs and personal devices

Managed Apple IDs can also be used with personally owned iOS devices and Mac computers. Students sign in to iCloud using the Managed Apple ID issued by the institution and an additional home-use password that serves as the second factor of the Apple ID two-factor authentication process. While using a Managed Apple ID on a personal device, iCloud Keychain isn't available, and the institution might restrict other features such as FaceTime or Messages. Any iCloud documents created by students when they are signed in are subject to audit as described previously in this section.

iMessage

Apple iMessage is a messaging service for iOS devices, Apple Watch, and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple doesn't log the contents of messages or attachments, which are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple can't decrypt the data.

When a user turns on iMessage on a device, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve for signing. The private keys for both key pairs are saved in the device's Keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which are verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. With some networks, this requires using SMS (the user will be presented with a confirmation dialog if the SMS is not zero rated). Phone number verification may be required for several system services in addition to iMessage, such as FaceTime and iCloud. All of the user's registered devices display an alert message when a new device, phone number, or email address is added.

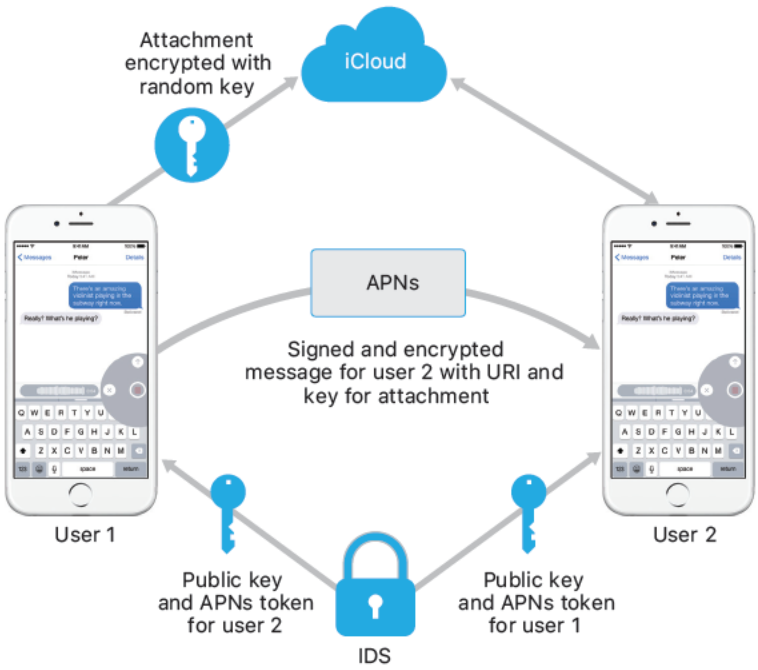
How iMessage sends and receives messages

Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the IDS to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. If the user enters a name, the device first utilizes the user's Contacts app to gather the phone numbers and email addresses associated with that name, then gets the public keys and APNs addresses from the IDS.

The user's outgoing message is individually encrypted for each of the receiver's devices. The public RSA encryption keys of the receiving devices are retrieved from IDS. For each receiving device, the sending device generates a random 88-bit value and uses it as an HMAC-SHA256 key to construct a 40-bit value derived from the sender and receiver

public key and the plaintext. The concatenation of the 88-bit and 40-bit values makes a 128-bit key, which encrypts the message with it using AES in CTR mode. The 40-bit value is used by the receiver side to verify the integrity of the decrypted plaintext. This per-message AES key is encrypted using RSA-OAEP to the public key of the receiving device. The combination of the encrypted message text and the encrypted message key is then hashed with SHA-1, and the hash is signed with ECDSA using the sending device's private signing key. The resulting messages, one for each receiving device, consist of the encrypted message text, the encrypted message key, and the sender's digital signature. They are then dispatched to the APNs for delivery. Metadata, such as the timestamp and APNs routing information, isn't encrypted. Communication with APNs is encrypted using a forward-secret TLS channel.

APNs can only relay messages up to 4KB or 16KB in size, depending on iOS version. If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using AES in CTR mode with a randomly generated 256-bit key and uploaded to iCloud. The AES key for the attachment, its URI (Uniform Resource Identifier), and a SHA-1 hash of its encrypted form are then sent to the recipient as the contents of an iMessage, with their confidentiality and integrity protected through normal iMessage encryption, as shown in the following diagram.



For group conversations, this process is repeated for each recipient and their devices.

On the receiving side, each device receives its copy of the message from APNs, and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's contacts so that a name can be displayed when possible.

As with all push notifications, the message is deleted from APNs when it is delivered. Unlike other APNs notifications, however, iMessage messages are queued for delivery to offline devices. Messages are currently stored for up to 30 days.

FaceTime

FaceTime is Apple's video and audio calling service. Similar to iMessage, FaceTime calls also use the Apple Push Notification service to establish an initial connection to the user's registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple can't decrypt the data.

The initial FaceTime connection is made through Apple server infrastructure that relays data packets between the users' registered devices. Using APNs notifications and Session Traversal Utilities for NAT (STUN) messages over the relayed connection, the devices verify their identity certificates and establish a shared secret for each session. The shared secret is used to derive session keys for media channels streamed via the Secure Real-time Transport Protocol (SRTP). SRTP packets are encrypted using AES-256 in Counter Mode and HMAC-SHA1. Subsequent to the initial connection and security setup, FaceTime uses STUN and Internet Connectivity Establishment (ICE) to establish a peer-to-peer connection between devices, if possible.

iCloud

iCloud stores a user's contacts, calendars, photos, documents, and more and keeps the information up to date across all of their devices, automatically. iCloud can also be used by third-party apps to store and sync documents as well as key values for app data as defined by the developer. Users set up iCloud by signing in with an Apple ID and choosing which services they would like to use. iCloud features, including My Photo Stream, iCloud Drive, and iCloud Backup, can be disabled by IT administrators via MDM configuration profiles. The service is agnostic about what is being stored and handles all file content the same way, as a collection of bytes.

Each file is broken into chunks and encrypted by iCloud using AES-128 and a key derived from each chunk's contents that utilizes SHA-256. The keys and the file's metadata are stored by Apple in the user's iCloud account. The encrypted chunks of the file are stored, without any user-identifying information, using third-party storage services, such as S3 and Google Cloud Platform.

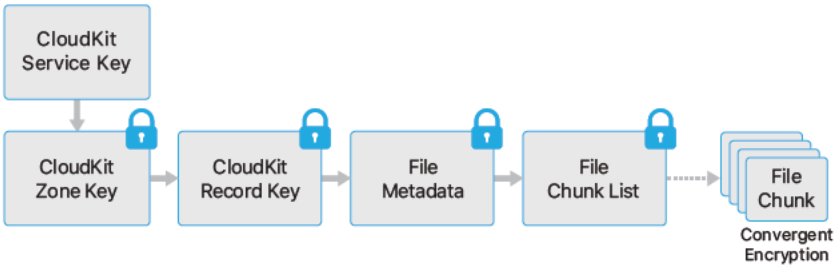
iCloud Drive

iCloud Drive adds account-based keys to protect documents stored in iCloud. As with existing iCloud services, it chunks and encrypts file contents and stores the encrypted chunks using third-party services. However, the file content keys are wrapped by record keys stored with the iCloud Drive metadata. These record keys are in turn protected by the user's iCloud Drive service key, which is then stored with the user's iCloud account. Users get access to their iCloud documents metadata by having authenticated with iCloud, but must also possess the iCloud Drive service key to expose protected parts of iCloud Drive storage.

CloudKit

CloudKit allows app developers to store key-value data, structured data, and assets in iCloud. Access to CloudKit is controlled using app entitlements. CloudKit supports both public and private databases. Public databases are used by all copies of the app, typically for general assets, and aren't encrypted. Private databases store the user's data.

As with iCloud Drive, CloudKit uses account-based keys to protect the information stored in the user's private database and, similar to other iCloud services, files are chunked, encrypted, and stored using third-party services. CloudKit utilizes a hierarchy of keys, similar to Data Protection. The per-file keys are wrapped by CloudKit Record keys. The Record keys, in turn, are protected by a zone-wide key, which is protected by the user's CloudKit Service key. The CloudKit Service key is stored in the user's iCloud account and is available only after the user has authenticated with iCloud.



CloudKit end-to-end encryption

Apple Pay Cash, User keywords, Siri Intelligence, and Hey Siri use CloudKit end-to-end encryption with a CloudKit service key protected by iCloud Keychain syncing. For these CloudKit containers, the key hierarchy is rooted in iCloud Keychain and therefore shares the security characteristics of iCloud Keychain—the keys are available only on the user's trusted devices, and not to Apple or any third party. If access to iCloud Keychain data is lost (see "Escrow security" section later in paper), the data in CloudKit is reset, and if data is available from the trusted local device it is re-uploaded to CloudKit.

iCloud Backup

iCloud also backs up information—including device settings, app data, photos, and videos in the Camera Roll, and conversations in the Messages app—daily over Wi-Fi. iCloud secures the content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. iCloud Backup occurs only when the device is locked, connected to a power source, and has Wi-Fi access to the Internet. Because of the encryption used in iOS, the system is designed to keep data secure while allowing incremental, unattended backup and restoration to occur.

Here's what iCloud backs up:

- Records for purchased music, movies, TV shows, apps, and books. A user's iCloud backup includes information about purchased content present on the user's iOS device, but not the purchased content itself. When the user restores from an iCloud backup, their purchased content is automatically downloaded from the iTunes Store, iBooks Store, or App Store. Some types of content aren't downloaded automatically in all countries or regions, and previous purchases may be unavailable if they have been refunded or are no longer available in the store. Full purchase history is associated with a user's Apple ID.
- Photos and videos on a user's iOS devices. Note that if a user turns on iCloud Photo Library on their iOS device (iOS 8.1 or later) or Mac (OS X 10.10.3 or later), their photos and videos are already stored in iCloud, so they aren't included in the user's iCloud backup.
- Contacts, calendar events, reminders, and notes
- Device settings
- App data
- Call history and ringtones
- Home screen and app organization
- HomeKit configuration
- HealthKit data
- iMessage, text (SMS), and MMS messages (requires the SIM card that was in use during backup)
- Visual Voicemail password (requires the SIM card that was in use during backup)

When files are created in Data Protection classes that aren't accessible when the device is locked, their per-file keys are encrypted using the class keys from the iCloud Backup keybag. Files are backed up to iCloud in their original, encrypted state. Files in Data Protection class No Protection are encrypted during transport.

The iCloud Backup keybag contains asymmetric (Curve25519) keys for each Data Protection class, which are used to encrypt the per-file keys. For more information about the contents of the backup keybag and the iCloud Backup keybag, see "Keychain Data Protection" in the Encryption and Data Protection section of this paper.

The backup set is stored in the user's iCloud account and consists of a copy of the user's files, and the iCloud Backup keybag. The iCloud Backup keybag is protected by a random key, which is also stored with the backup set. (The user's iCloud password isn't utilized for encryption so changing the iCloud password won't invalidate existing backups.)

While the user's Keychain database is backed up to iCloud, it remains protected by a UID-tangled key. This allows the Keychain to be restored only to the same device from which it originated, and it means no one else, including Apple, can read the user's Keychain items.

On restore, the backed-up files, iCloud Backup keybag, and the key for the keybag are retrieved from the user's iCloud account. The iCloud Backup keybag is decrypted using its key, then the per-file keys in the keybag are used to decrypt the files in the backup set, which are written as new files to the file system, thus re-encrypting them as per their Data Protection class.

Safari integration with iCloud Keychain
Safari can automatically generate cryptographically strong random strings for website passwords, which are stored in Keychain and synced to other devices. Keychain items are transferred from device to device, traveling through Apple servers, but are encrypted in such a way that Apple and other devices can't read their contents.

iCloud Keychain

iCloud Keychain allows users to securely sync their passwords between iOS devices and Mac computers without exposing that information to Apple. In addition to strong privacy and security, other goals that heavily influenced the design and architecture of iCloud Keychain were ease of use and the ability to recover a Keychain. iCloud Keychain consists of two services: Keychain syncing and Keychain recovery.

Apple designed iCloud Keychain and Keychain recovery so that a user's passwords are still protected under the following conditions:

- A user's iCloud account is compromised.
- iCloud is compromised by an external attacker or employee.
- A third party accesses user accounts.

Keychain syncing

When a user enables iCloud Keychain for the first time, the device establishes a circle of trust and creates a syncing identity for itself. The syncing identity consists of a private key and a public key. The public key of the syncing identity is put in the circle, and the circle is signed twice: first by the private key of the syncing identity, then again with an asymmetric elliptical key (using P-256) derived from the user's iCloud account password. Also stored with the circle are the parameters (random salt and iterations) used to create the key that is based on the user's iCloud password.

The signed syncing circle is placed in the user's iCloud key value storage area. It can't be read without knowing the user's iCloud password, and can't be modified validly without having the private key of the syncing identity of its member.

When the user turns on iCloud Keychain on another device, it notices that the user has a previously established syncing circle in iCloud that it isn't a member of. The device creates its syncing identity key pair, then creates an application ticket to request membership in the circle. The ticket consists of the device's public key of its syncing identity, and the user is asked to authenticate with their iCloud password. The elliptical key generation parameters are retrieved from iCloud and generate a key that is used to sign the application ticket. Finally, the application ticket is placed in iCloud.

When the first device sees that an application ticket has arrived, it displays a notice for the user to acknowledge that a new device is asking to join the syncing circle. The user enters their iCloud password, and the application ticket is verified as signed by a matching private key. This establishes that the person who generated the request to join the circle entered the user's iCloud password at the time the request was made.

Upon the user's approval to add the new device to the circle, the first device adds the public key of the new member to the syncing circle, signs it again with both its syncing identity and the key derived from the user's iCloud password. The new syncing circle is placed in iCloud, where it is similarly signed by the new member of the circle.

There are now two members of the signing circle, and each member has the public key of its peer. They now begin to exchange individual Keychain items via iCloud key value storage or store them in CloudKit as appropriate. If both circle members have the same item, the one with the most recent modification date will be synced. Items are skipped if

the other member has the item and the modification dates are identical. Each item that's synced is encrypted so it can be decrypted only by a device within the user's circle of trust. It can't be decrypted by any other devices or Apple.

This process is repeated as new devices join the syncing circle. For example, when a third device joins, the confirmation appears on both of the other user's devices. The user can approve the new member from either of those devices. As new peers are added, each peer syncs with the new one to ensure that all members have the same Keychain items.

However, the entire Keychain isn't synced. Some items are device-specific, such as VPN identities, and shouldn't leave the device. Only items with the attribute `kSecAttrSynchronizable` are synced. Apple has set this attribute for Safari user data (including user names, passwords, and credit card numbers), as well as Wi-Fi passwords and HomeKit encryption keys.

Additionally, by default, Keychain items added by third-party apps don't sync. Developers must set the `kSecAttrSynchronizable` when adding items to the Keychain.

Keychain recovery

Keychain recovery provides a way for users to optionally escrow their Keychain with Apple, without allowing Apple to read the passwords and other data it contains. Even if the user has only a single device, Keychain recovery provides a safety net against data loss. This is particularly important when Safari is used to generate random, strong passwords for web accounts, as the only record of those passwords is in the Keychain.

A cornerstone of Keychain recovery is secondary authentication and a secure escrow service, created by Apple specifically to support this feature. The user's Keychain is encrypted using a strong passcode, and the escrow service will provide a copy of the Keychain only if a strict set of conditions are met.

When iCloud Keychain is turned on, if two-factor authentication is enabled for the user's account, the device passcode will be used to recover an escrowed Keychain. If two-factor authentication isn't set up, the user is asked to create an iCloud Security Code by providing a six-digit passcode. Alternatively, without two-factor authentication, users can specify their own longer code, or let their devices create a cryptographically random code that they can record and keep on their own.

Next, the iOS device exports a copy of the user's Keychain, encrypts it wrapped with keys in an asymmetric keybag, and places it in the user's iCloud key value storage area. The keybag is wrapped with the user's iCloud Security Code and the public key of the hardware security module (HSM) cluster that will store the escrow record. This becomes the user's iCloud Escrow Record.

If the user decides to accept a cryptographically random security code, instead of specifying their own or using a four-digit value, no escrow record is necessary. Instead, the iCloud Security Code is used to wrap the random key directly.

In addition to establishing a security code, users must register a phone number. This provides a secondary level of authentication during Keychain recovery. The user will receive an SMS that must be replied to in order for the recovery to proceed.

Escrow security

iCloud provides a secure infrastructure for Keychain escrow that ensures only authorized users and devices can perform a recovery. Topographically positioned behind iCloud are HSM clusters that guard the escrow records. Each has a key that is used to encrypt the escrow records under their watch, as described previously in this paper.

To recover a Keychain, users must authenticate with their iCloud account and password and respond to an SMS sent to their registered phone number. Once this is done, users must enter their iCloud Security Code. The HSM cluster verifies that a user knows their iCloud Security Code using the Secure Remote Password (SRP) protocol; the code itself isn't sent to Apple. Each member of the cluster independently verifies that the user hasn't exceeded the maximum number of attempts allowed to retrieve their record, as discussed below. If a majority agree, the cluster unwraps the escrow record and sends it to the user's device.

Next, the device uses the iCloud Security Code to unwrap the random key used to encrypt the user's Keychain. With that key, the Keychain—retrieved from iCloud key value storage—is decrypted and restored onto the device. Only 10 attempts to authenticate and retrieve an escrow record are allowed. After several failed attempts, the record is locked and the user must call Apple Support to be granted more attempts. After the 10th failed attempt, the HSM cluster destroys the escrow record and the Keychain is lost forever. This provides protection against a brute-force attempt to retrieve the record, at the expense of sacrificing the Keychain data in response.

These policies are coded in the HSM firmware. The administrative access cards that permit the firmware to be changed have been destroyed. Any attempt to alter the firmware or access the private key will cause the HSM cluster to delete the private key. Should this occur, the owner of each Keychain protected by the cluster will receive a message informing them that their escrow record has been lost. They can then choose to re-enroll.

Siri

By simply talking naturally, users can enlist Siri to send messages, schedule meetings, place phone calls, and more. Siri uses speech recognition, text-to-speech, and a client-server model to respond to a broad range of requests. The tasks that Siri supports have been designed to ensure that only the absolute minimal amount of personal information is utilized and that it is fully protected.

When Siri is turned on, the device creates random identifiers for use with the voice recognition and Siri servers. These identifiers are used only within Siri and are utilized to improve the service. If Siri is subsequently turned off, the device will generate a new random identifier to be used if Siri is turned back on.

To facilitate Siri features, some of the user's information from the device is sent to the server. This includes information about the music library (song titles, artists, and playlists), the names of Reminders lists, and names and relationships that are defined in Contacts. All communication with the server is over HTTPS.

When a Siri session is initiated, the user's first and last name (from Contacts), along with a rough geographic location, are sent to the server. This allows Siri to respond with the name or answer questions that need only an approximate location, such as those about the weather.

If a more precise location is necessary—such as determining the location of nearby movie theaters—the server asks the device to provide a more exact location. This is an example of how, by default, information is sent to the server only when it's strictly necessary to process the user's request. In any event, session information is discarded after 10 minutes of inactivity.

When Siri is used from Apple Watch, the watch creates its own random unique identifier, as described previously. However, instead of sending the user's information again, its requests also send the Siri identifier of the paired iPhone to provide a reference to that information.

The recording of the user's spoken words is sent to Apple's voice recognition server. If the task involves dictation only, the recognized text is sent back to the device. Otherwise, Siri analyzes the text and, if necessary, combines it with information from the profile associated with the device. For example, if the request is "send a message to my mom," the relationships and names that were uploaded from Contacts are utilized. The command for the identified action is then sent back to the device to be carried out.

Many Siri functions are accomplished by the device under the direction of the server. For example, if the user asks Siri to read an incoming message, the server simply tells the device to speak the contents of its unread messages. The contents and sender of the message aren't sent to the server.

User voice recordings are saved for a six-month period so that the recognition system can utilize them to better understand the user's voice. After six months, another copy is saved, without its identifier, for use by Apple in improving and developing Siri for up to two years. A small subset of recordings, transcripts, and associated data without identifiers may continue to be used by Apple for ongoing improvement and quality assurance of Siri beyond two years. Additionally, some recordings that reference music, sports teams and players, and businesses or points of interest are similarly saved for purposes of improving Siri.

Siri can also be invoked hands-free via voice activation. The voice trigger detection is performed locally on the device. In this mode, Siri is activated only when the incoming audio pattern sufficiently matches the acoustics of the specified trigger phrase. When the trigger is detected, the corresponding audio including the subsequent Siri command is sent to Apple's voice recognition server for further processing, which follows the same rules as other user voice recordings made through Siri.

Continuity

Continuity takes advantage of technologies like iCloud, Bluetooth, and Wi-Fi to enable users to continue an activity from one device to another; make and receive phone calls; send and receive text messages; and share a cellular Internet connection.

Handoff

With Handoff, when a user's Mac and iOS devices are near each other, the user can automatically pass whatever they're working on from one device to the other. Handoff lets the user switch devices and instantly continue working.

When a user signs in to iCloud on a second Handoff capable device, the two devices establish a Bluetooth Low Energy 4.0 pairing out-of-band using APNs. The individual messages are encrypted in a similar fashion to iMessage. Once the devices are paired, each will generate a symmetric 256-bit AES key that gets stored in the device's Keychain. This key can encrypt and authenticate the Bluetooth Low Energy advertisements that communicate the device's current activity to other iCloud paired devices using AES-256 in GCM mode, with replay protection measures. The first time a device receives an advertisement from a new key, it will establish a Bluetooth Low Energy connection to the originating device and perform an advertisement encryption key exchange. This connection is secured using standard Bluetooth Low Energy 4.0 encryption as well as encryption of the individual messages, which is similar to how iMessage is encrypted. In some situations, these messages will go via APNs instead of Bluetooth Low Energy. The activity payload is protected and transferred in the same way as an iMessage.

Handoff between native apps and websites

Handoff allows an iOS native app to resume web pages in domains legitimately controlled by the app developer. It also allows the native app user activity to be resumed in a web browser.

To prevent native apps from claiming to resume websites not controlled by the developer, the app must demonstrate legitimate control over the web domains it wants to resume. Control over a website domain is established via the mechanism for shared web credentials. For details, refer to "Access to Safari saved passwords" in the Encryption and Data Protection section of this paper. The system must validate an app's domain name control before the app is permitted to accept user activity Handoff.

The source of a web page Handoff can be any browser that has adopted the Handoff APIs. When the user views a web page, the system advertises the domain name of the web page in the encrypted Handoff advertisement bytes. Only the user's other devices can decrypt the advertisement bytes (as described earlier in this section).

On a receiving device, the system detects that an installed native app accepts Handoff from the advertised domain name and displays that native app icon as the Handoff option. When launched, the native app receives the full URL and the title of the web page. No other information is passed from the browser to the native app.

In the opposite direction, a native app may specify a fallback URL when a Handoff receiving device doesn't have the same native app installed. In this case, the system displays the user's default browser as the Handoff app option (if that browser has adopted Handoff APIs). When Handoff

is requested, the browser will be launched and given the fallback URL provided by the source app. There is no requirement that the fallback URL be limited to domain names controlled by the native app developer.

Handoff of larger data

In addition to the basic feature of Handoff, some apps may elect to use APIs that support sending larger amounts of data over Apple-created peer-to-peer Wi-Fi technology (in a similar fashion to AirDrop). For example, the Mail app uses these APIs to support Handoff of a mail draft, which may include large attachments.

When an app uses this facility, the exchange between the two devices starts off just as in Handoff (see previous sections). However, after receiving the initial payload using Bluetooth Low Energy, the receiving device initiates a new connection over Wi-Fi. This connection is encrypted (TLS), which exchanges their iCloud identity certificates. The identity in the certificates is verified against the user's identity. Further payload data is sent over this encrypted connection until the transfer completes.

Universal Clipboard

Universal Clipboard leverages Handoff to securely transfer the content of a user's clipboard across devices so they can copy on one device and paste on another. Content is protected the same way as other Handoff data and shared by default with Universal Clipboard, unless the app developer chooses to disallow sharing.

Apps have access to clipboard data regardless of whether the user has pasted the clipboard into the app. With Universal Clipboard, this data access extends to apps running on the user's other devices (as established by their iCloud sign-in).

Auto Unlock

Mac computers that support Auto Unlock use Bluetooth Low Energy and peer-to-peer Wi-Fi to securely allow the user's Apple Watch to unlock their Mac. Each capable Mac and Apple Watch associated with an iCloud account must use two-factor authorization (TFA).

When enabling an Apple Watch to unlock a Mac, a secure link using Auto Unlock Identities is established. The Mac creates a random one-time-use unlock secret and transmits it to the Apple Watch over the link. The secret is stored on Apple Watch and can only be accessed when Apple Watch is unlocked (see "Data Protection classes" section). Neither the master entropy nor the new secret is the user's password.

During an unlock operation, the Mac uses Bluetooth Low Energy to create a connection to the Apple Watch. A secure link is then established between the two devices using the shared keys used when it was first enabled. The Mac and Apple Watch then use peer-to-peer Wi-Fi and a secure key derived from the secure link to determine the distance between the two devices. If the devices are within range, the secure link is then used to transfer the pre-shared secret to unlock the Mac. After successful unlock, the Mac replaces the current unlock secret with a new one-time use unlock secret and transmits the new unlock secret to the Apple Watch over the link.

iPhone Cellular Call Relay

When a user's Mac, iPad, or iPod touch is on the same Wi-Fi network as their iPhone, it can make and receive phone calls using the cellular connection on iPhone. Configuration requires the devices to be signed in to both iCloud and FaceTime using the same Apple ID account.

When an incoming call arrives, all configured devices will be notified via the Apple Push Notification service, with each notification using the same end-to-end encryption as iMessage. Devices that are on the same network will present the incoming call notification UI. Upon answering the call, the audio is seamlessly transmitted from the user's iPhone using a secure peer-to-peer connection between the two devices.

When a call is answered on one device, ringing of nearby iCloud-paired devices is terminated by briefly advertising via Bluetooth Low Energy 4.0. The advertising bytes are encrypted using the same method as Handoff advertisements.

Outgoing calls are also relayed to iPhone via the Apple Push Notification service, and audio will be similarly transmitted over the secure peer-to-peer link between devices.

Users can disable phone call relay on a device by turning off iPhone Cellular Calls in FaceTime settings.

iPhone Text Message Forwarding

Text Message Forwarding automatically sends SMS text messages received on an iPhone to a user's enrolled iPad, iPod touch, or Mac. Each device must be signed in to the iMessage service using the same Apple ID account. When Text Message Forwarding is turned on, enrollment is automatic on devices within a user's circle of trust if two-factor authentication is enabled. Otherwise, enrollment is verified on each device by entering a random six-digit numeric code generated by iPhone.

Once devices are linked, iPhone encrypts and forwards incoming SMS text messages to each device, utilizing the methods described in the iMessage section of this paper. Replies are sent back to iPhone using the same method, then iPhone sends the reply as a text message using the carrier's SMS transmission mechanism. Text Message Forwarding can be turned on or off in Messages settings.

Instant Hotspot

iOS devices that support Instant Hotspot use Bluetooth Low Energy to discover and communicate to devices that have signed in to the same iCloud account. Compatible Mac computers running OS X Yosemite or later use the same technology to discover and communicate with Instant Hotspot iOS devices.

When a user enters Wi-Fi Settings on the iOS device, the device emits a Bluetooth Low Energy signal containing an identifier that all devices signed in to the same iCloud account agree upon. The identifier is generated from a DSID (Destination Signaling Identifier) tied to the iCloud account, and rotated periodically. When other devices signed in to the same iCloud account are in close proximity and support Personal Hotspot, they detect the signal and respond, indicating availability.

When a user chooses a device available for Personal Hotspot, a request to turn on Personal Hotspot is sent to that device. The request is sent across a link that is encrypted using standard Bluetooth Low Energy encryption, and the request is encrypted in a fashion similar to iMessage

encryption. The device then responds across the same Bluetooth Low Energy link using the same per-message encryption with Personal Hotspot connection information.

Safari Suggestions, Siri Suggestions in Search, Lookup, #images, News App, and News Widget in Non-News Countries

Safari Suggestions, Siri Suggestions in Search, Lookup, #images, News app, and News widget in non-News countries show users suggestions that go beyond their devices, from sources like Wikipedia, the iTunes Store, local News, Maps results, and the App Store—and even offer suggestions before a user begins typing.

When a user starts typing in the Safari address bar, opens or uses Siri Suggestions in Search, uses Lookup, opens #images, uses Search in the News app, or uses the News widget in non-News countries, the following context is sent encrypted using HTTPS to Apple to provide the user with relevant results:

- An identifier that rotates every 15 minutes to preserve privacy
- User's search query
- The most likely query completion based on context and locally cached past searches
- The approximate location of their device, if they have Location Services for Location-Based Suggestions turned on. The level of location "blurring" is based on estimated population density at the device's location; for instance, more blurring in a rural location where users may be geographically more separated versus less blurring in a city center where users will typically be closer together. Users can disable the sending of all location information to Apple in Settings, by turning off Location Services for Location-Based Suggestions. If Location Services is turned off, then Apple may use the device's IP address to infer an approximate location.
- The type of device and whether the search is made in Siri Suggestions in Search, Safari, Lookup, News App, or Messages
- The type of connection
- Information on the three apps most recently used on the device (for additional search context). Only apps that are in an Apple-maintained allow list of popular apps and have been accessed within the last 3 hours are included.
- A list of popular applications on the device
- Regional language, locale, and input preferences
- If the user's device can access music or video subscription services, then information such as names of the subscription services and types of subscriptions may be sent to Apple. The user's account name, number, and password aren't sent to Apple.
- Summarized, aggregated representation of topics of interests

When a user selects a result or exits the app with no result selected, some information is sent to Apple to help improve the quality of future results. This information is tied only to the same 15-minute session identifier and not tied to a particular user. The feedback includes some of the previously described context information as well as interaction information such as:

- Timings between interactions and search network requests
- Ranking and display order of suggestions
- The ID of the result and action selected if result is non-local, or the category of the result selected if it is local
- A flag indicating whether the user selected the result

Apple retains Suggestions logs with queries, context, and feedback for 18 months. A subset of logs are retained for up to five years; for example queries, locale, domain, approximate location, and aggregate metrics.

In some cases, Suggestions may forward queries for common words and phrases to a qualified partner, in order to receive and display the partner's search results. Apple proxies the queries so that partners don't receive user IP addresses or search feedback. Communication with the partner is encrypted via HTTPS. For queries that occur frequently, Apple provides city-level location, device type, and client language as search context to the partner to improve search performance. In iOS 11, Siri Suggestions in Search queries aren't sent to partners.

To understand and improve Suggestions performance geographically and across different types of networks, the following information is logged without a session identifier:

- Partial IP address (without the last octet for IPv4 addresses; without the last 80 bits for IPv6 addresses)
- Approximate location
- Approximate time of the query
- Latency/transfer rate
- Response size
- Connection type
- Locale
- Device type and requesting app

Device Controls

iOS supports flexible security policies and configurations that are easy to enforce and manage. This enables organizations to protect corporate information and ensure that employees meet enterprise requirements, even if they are using devices they've provided themselves—for example, as part of a "bring your own device" (BYOD) program.

Organizations can use resources such as passcode protection, configuration profiles, remote wipe, and third-party MDM solutions to manage fleets of devices and help keep corporate data secure, even when employees access this data on their personal iOS devices.

Passcode protection

By default, the user's passcode can be defined as a numeric PIN. On devices with Touch ID or Face ID, the minimum passcode length is six digits. On other devices, the minimum length is four digits. Users can specify a longer alphanumeric passcode by selecting Custom Alphanumeric Code in the Passcode Options in Settings > Passcode. Longer and more complex passcodes are harder to guess or attack, and are recommended.

Administrators can enforce complex passcode requirements and other policies using MDM or Exchange ActiveSync, or by requiring users to manually install configuration profiles. The following passcode policies are available:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts
- Allow Touch ID or Face ID

For administrator details about each policy, go to: https://help.apple.com/deployment/ios/#/apd4D6A472A-A494-4DFD-B559-D59E63167E43

For developer details about each policy, go to: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

iOS pairing model

iOS uses a pairing model to control access to a device from a host computer. Pairing establishes a trust relationship between the device and its connected host, signified by public key exchange. iOS uses this sign of trust to enable additional functionality with the connected host, such as data synchronization.

In iOS 9, services that require pairing can't be started until after the device has been unlocked by the user.

Additionally in iOS 10, some services, including photo syncing, require the device to be unlocked to begin.

Beginning in iOS 11, services won't start unless the device has been recently unlocked.

The pairing process requires the user to unlock the device and accept the pairing request from the host. Starting in iOS 11, the user is also required to enter their passcode. After the user has done this, the host and device exchange and save 2048-bit RSA public keys. The host is then given a 256-bit key that can unlock an escrow keybag stored on the device (refer to "Escrow keybag" within the "Keybags" section of this paper). The exchanged keys are used to start an encrypted SSL session, which the device requires before it will send protected data to the host or start a service (iTunes syncing, file transfers, Xcode development, etc.). The device requires connections from a host over Wi-Fi to use this encrypted session for all communication, so it must have been previously paired over USB. Pairing also enables several diagnostic capabilities. In iOS 9, if a pairing record hasn't been used for more than six months, it expires. This timeframe is shortened to 30 days in iOS 11.

For more information, go to:
https://support.apple.com/kb/HT6331

Certain services, including com.apple.pcapd, are restricted to work only over USB. Additionally, the com.apple.file_relay service requires an Apple-signed configuration profile to be installed.

In iOS 11, Apple TV can to use the Secure Remote Password protocol to wirelessly establish a pairing relationship.

A user can clear the list of trusted hosts with the "Reset Network Settings" or "Reset Location & Privacy" options.

For more information, go to:
https://support.apple.com/kb/HT5868

Configuration enforcement

A configuration profile is an XML file that allows an administrator to distribute configuration information to iOS devices. Settings that are defined by an installed configuration profile can't be changed by the user. If the user deletes a configuration profile, all the settings defined by the profile are also removed. In this manner, administrators can enforce settings by tying policies to Wi-Fi and data access. For example, a

configuration profile that provides an email configuration can also specify a device passcode policy. Users won't be able to access mail unless their passcode meets the administrator's requirements.

An iOS configuration profile contains a number of settings that can be specified, including:

- Passcode policies
- Restrictions on device features (disabling the camera, for example)
- Wi-Fi settings
- VPN settings
- Mail server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys
- Advanced cellular network settings

To view a current list for administrators, go to:
https://help.apple.com/deployment/ios/#/cad5370d089

To view a current list for developers, go to:
https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

Configuration profiles can be signed and encrypted to validate their origin, ensure their integrity, and protect their contents. Configuration profiles are encrypted using CMS (RFC 3852), supporting 3DES and AES-128.

Configuration profiles can also be locked to a device to completely prevent their removal, or to allow removal only with a passcode. Since many enterprise users own their iOS devices, configuration profiles that bind a device to an MDM solution can be removed—but doing so also removes all managed configuration information, data, and apps.

Users can install configuration profiles directly on their devices using Apple Configurator 2, or they can be downloaded via Safari, sent via a mail message, or sent over the air using an MDM solution. When a user sets up a device in the Device Enrollment Program or Apple School Manager, the device downloads and installs a profile for MDM enrollment.

Mobile device management (MDM)

iOS support for MDM allows businesses to securely configure and manage scaled iPhone, iPad, Apple TV, and Mac deployments across their organizations. MDM capabilities are built on existing iOS technologies such as configuration profiles, over-the-air enrollment, and the Apple Push Notification service. For example, APNs is used to wake the device so it can communicate directly with its MDM solution over a secured connection. No confidential or proprietary information is transmitted via APNs.

Using MDM, IT departments can enroll iOS devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed devices.

For more information on MDM, go to:
https://www.apple.com/iphone/business/it/management.html

Shared iPad

Shared iPad is a multi-user mode for use in educational iPad deployments. It allows students to share an iPad without sharing documents and data. Each student gets their own home directory, which is created as an APFS volume protected by the user's credential. Shared iPad requires the use of a Managed Apple ID that is issued and owned by the school. Shared iPad enables a student to sign in to any organizationally owned device that is configured for use by multiple students.

Student data is partitioned into separate home directories, each in their own data protection domains and protected by both UNIX permissions and sandboxing. When a student signs in, the Managed Apple ID is authenticated with Apple's identity servers using the SRP protocol. If successful, a short-lived access token specific to the device is granted. If the student has used the device before, they already have a local user account that is unlocked using the same credential. If the student hasn't used the device before, a new UNIX user ID, an APFS volume with the user's home directory, and a logical Keychain are provisioned. If the device isn't connected to the Internet (say, because the student is on a field trip), authentication can occur against the local account for a limited number of days. In that situation, only users with previously existing local accounts can sign in. Once the time limit has expired, students are required to authenticate online, even if a local account already exists.

After the student's local account has been unlocked or created, if it is remotely authenticated, the short-lived token issued by Apple's servers is converted to an iCloud token that permits signing in to iCloud. Next, the student's settings are restored and their documents and data are synced from iCloud.

While the student session is active and the device remains online, documents and data are stored on iCloud as they are created or modified. In addition, a background syncing mechanism ensures that changes are pushed to iCloud after the student signs out. Once background syncing for that user is complete, the user's APFS volume is unmounted and can't be mounted again without supplying the user's credentials.

When a Shared iPad is upgraded from a version prior to iOS 10.3 to a version of 10.3 or later, a one-time file system conversion takes place to convert the HFS+ data partition to an APFS volume. If, at that time, any user home directories are present on the system, they will remain on the main data volume instead of being converted to individual APFS volumes. When additional students sign in, their home directories will also be placed on the main data volume. New user accounts won't be created with their own APFS volume, as described previously, until all user accounts on the main data volume have been deleted. Thus, to ensure that users have the additional protections and quotas afforded by APFS, the iPad should either be upgraded to 10.3 or later via an erase-and-re-install, or all user accounts on the device should be deleted via the Delete User MDM command.

Apple School Manager

Apple School Manager is a service for educational institutions that enables them to buy content, configure automatic device enrollment in MDM solutions, create accounts for students and staff, and set up iTunes U courses. Apple School Manager is accessible on the web and is designed for technology managers and IT administrators, staff, and teachers.

For more information on Apple School Manager, go to:
https://help.apple.com/schoolmanager/

Device Enrollment

The Device Enrollment Program (DEP), part of Apple School Manager and Apple Deployment Programs, provides a fast, streamlined way to deploy iOS devices that an organization has purchased directly from Apple or through participating Apple Authorized Resellers and carriers. iOS devices running iOS 11 or later can also be added to DEP after the time of purchase using Apple Configurator 2.

Organizations can automatically enroll devices in MDM without having to physically touch or prep the devices before users get them. After enrolling in the program, administrators sign in to the program website and link the program to their MDM solution. The devices they purchased can then be assigned to users via MDM. Once a user has been assigned, any MDM-specified configurations, restrictions, or controls are automatically installed. All communications between devices and Apple servers are encrypted in transit via HTTPS (SSL).

The setup process for users can be further simplified by removing specific steps in the Setup Assistant, so users are up and running quickly. Administrators can also control whether or not the user can remove the MDM profile from the device and ensure that device restrictions are in place from the very start. Once the device is unboxed and activated, it can enroll in the organization's MDM solution—and all management settings, apps, and books are installed.

For more information related to businesses, go to:
https://help.apple.com/deployment/business/

For more information related to educational institutions, go to:
https://help.apple.com/schoolmanager/

Note: Device enrollment isn't available in all countries or regions.

Apple Configurator 2

In addition to MDM, Apple Configurator 2 for macOS makes it easy to set up and preconfigure iOS devices and Apple TV before handing them out to users. With Apple Configurator 2, devices can be quickly preconfigured with apps, data, restrictions, and settings.

Apple Configurator 2 allows you to use Apple School Manager (for education) or the Device Enrollment Program (for business) to enroll devices in an MDM solution without users having to use the Setup Assistant. Apple Configurator 2 can also be used to add iOS devices and Apple TV to Apple School Manager or the Device Enrollment Program after the time of purchase.

For more information on Apple Configurator 2, go to:
https://help.apple.com/configurator/mac/

Supervision

During the setup of a device, an organization can configure the device to be supervised. Supervision denotes that the device is institutionally owned, which provides additional control over its configuration and restrictions. Devices can be supervised during setup through Apple School Manager, the Device Enrollment Program, or Apple Configurator 2. Supervising a device requires the device to be erased and the operating system reinstalled.

For more information on configuring and managing devices using MDM or Apple Configurator 2, go to:
https://help.apple.com/deployment/ios/

Restrictions

Restrictions can be enabled—or in some cases, disabled—by administrators to prevent users from accessing a specific app, service, or function of the device. Restrictions are sent to devices in a restrictions payload, which is attached to a configuration profile. Restrictions can be applied to iOS, tvOS, and macOS devices. Certain restrictions on a managed iPhone may be mirrored on a paired Apple Watch.

To view a current list for IT managers, go to:
https://help.apple.com/deployment/ios/#/apdbd6309354

Remote wipe

iOS devices can be erased remotely by an administrator or user. Instant remote wipe is achieved by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. A remote wipe command can be initiated by MDM, Exchange, or iCloud.

When a remote wipe command is triggered by MDM or iCloud, the device sends an acknowledgment and performs the wipe. For remote wipe via Exchange, the device checks in with the Exchange server before performing the wipe.

Users can also wipe devices in their possession using the Settings app. And as mentioned, devices can be set to automatically wipe after a series of failed passcode attempts.

Lost Mode

If a device is lost or stolen, an MDM administrator can remotely enable Lost Mode on a supervised device with iOS 9.3 or later. When Lost Mode is enabled, the current user is logged out and the device can't be unlocked. The screen displays a message that can be customized by the administrator, such as displaying a phone number to call if the device is found. When the device is put into Lost Mode, the administrator can request the device to send its current location and, optionally, play a sound. When an administrator turns off Lost Mode, which is the only way the mode can be exited, the user is informed of this action through a message on the Lock screen or an alert on the Home screen.

Activation Lock

When Find My iPhone is turned on, the device can't be reactivated without entering the owner's Apple ID credentials or the previous passcode of the device.

With devices that are owned by an organization, it's a good idea to supervise devices so that Activation Lock can be managed by the organization instead of relying on the individual user to enter their Apple ID credentials to reactivate devices.

On supervised devices, a compatible MDM solution can store a bypass code when Activation Lock is enabled, or later use this code to clear Activation Lock automatically when the device needs to be erased and assigned to a new user.

By default, supervised devices never have Activation Lock enabled, even if the user turns on Find My iPhone. However, an MDM solution may retrieve a bypass code and permit Activation Lock to be enabled on the device. If Find My iPhone is turned on when the MDM solution enables Activation Lock, it is enabled at that point. If Find My iPhone is turned off when the MDM server enables Activation Lock, it's enabled the next time the user activates Find My iPhone.

For devices used in education with a Managed Apple ID created through Apple School Manager, Activation Lock can be tied to an administrator's Apple ID rather than the user's Apple ID, or disabled using the device's bypass code.

Privacy Controls

Apple takes customer privacy seriously and has numerous built-in controls and options that allow iOS users to decide how and when apps utilize their information, as well as what information is being utilized.

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine the user's approximate location. Location Services can be turned off using a single switch in Settings, or users can approve access for each app that uses the service. Apps may request to receive location data only while the app is being used or allow it at any time. Users may choose not to allow this access, and may change their choice at any time in Settings. From Settings, access can be set to never allowed, allowed when in use, or always, depending on the app's requested location use. Also, if apps granted access to use location at any time make use of this permission while in background mode, users are reminded of their approval and may change an app's access.

Additionally, users are given fine-grained control over system services' use of location information. This includes being able to turn off the inclusion of location information in information collected by the analytics services used by Apple to improve iOS, location-based Siri information, location-based context for Siri Suggestions searches, local traffic conditions, and significant locations visited in the past.

Access to personal data

iOS helps prevent apps from accessing a user's personal information without permission. Additionally, in Settings, users can see which apps they have permitted to access certain information, as well as grant or revoke any future access. This includes access to:

- Contacts
- Calendars
- Reminders
- Photos
- Motion activity and fitness
- Location Services
- Apple Music
- Your music and video activity
- Social media accounts, such as Twitter and Facebook
- Microphone
- Camera
- HomeKit
- Health
- Speech recognition
- Bluetooth sharing
- Your media library

If the user signs in to iCloud, apps are granted access by default to iCloud Drive. Users may control each app's access under iCloud in Settings. Additionally, iOS provides restrictions that prevent data movement between apps and accounts installed by an MDM solution and those installed by the user.

Privacy policy

To read Apple's privacy policy, go to:
https://www.apple.com/legal/privacy

Apple Security Bounty

Apple rewards researchers who share critical issues with Apple. In order to be eligible for an Apple Security Bounty, researchers are required to provide a clear report and working proof of concept. The vulnerability must affect the latest shipping iOS and, where relevant, the latest hardware. The exact payment amount will be determined after review by Apple. The criteria includes novelty, likelihood of exposure, and degree of user interaction required.

Once the issues are properly shared, Apple makes it a priority to resolve confirmed issues as quickly as possible. Where appropriate, Apple will provide public recognition, unless otherwise requested.

Category	Maximum payment (USD)
Secure boot firmware components	$200,000
Extraction of confidential material protected by the Secure Enclave	$100,000
Execution of arbitrary code with kernel privileges	$50,000
Unauthorized access to iCloud account data on Apple servers	$50,000
Access from a sandboxed process to user data outside of that sandbox	$25,000

Conclusion

A commitment to security

Apple is committed to helping protect customers with leading privacy and security technologies that are designed to safeguard personal information, as well as comprehensive methods to help protect corporate data in an enterprise environment.

Security is built into iOS. From the platform to the network to the apps, everything a business needs is available in the iOS platform. Together, these components give iOS its industry-leading security without compromising the user experience.

Apple uses a consistent, integrated security infrastructure throughout iOS and the iOS apps ecosystem. Hardware-based storage encryption provides remote wipe capabilities when a device is lost, and enables users to completely remove all corporate and personal information when a device is sold or transferred to another owner. Diagnostic information is also collected anonymously.

iOS apps designed by Apple are built with enhanced security in mind. For example, iMessage and FaceTime provide client-to-client encryption. For

third-party apps, the combination of required code signing, sandboxing, and entitlements gives users industry-leading protection against viruses, malware, and other exploits. The App Store submission process works to further shield users from these risks by reviewing every iOS app before it's made available.

To make the most of the extensive security features built into iOS, businesses are encouraged to review their IT and security policies to ensure that they are taking full advantage of the layers of security technology offered by this platform.

Apple maintains a dedicated security team to support all Apple products. The team provides security auditing and testing for products under development, as well as for released products. The Apple team also provides security tools and training, and actively monitors for reports of new security issues and threats. Apple is a member of the Forum of Incident Response and Security Teams (FIRST).

To learn more about reporting issues to Apple and subscribing to security notifications, go to:
https://www.apple.com/support/security

Glossary

Address space layout randomization (ASLR)	A technique employed by iOS to make the successful exploitation by a software bug much more difficult. By ensuring memory addresses and offsets are unpredictable, exploit code can't hard code these values. In iOS 5 or later, the position of all system apps and libraries are randomized, along with all third-party apps compiled as position-independent executables.
Apple Push Notification service (APNs)	A worldwide service provided by Apple that delivers push notifications to iOS devices.
Boot ROM	The very first code executed by a device's processor when it first boots. As an integral part of the processor, it can't be altered by either Apple or an attacker.
Data Protection	File and Keychain protection mechanism for iOS. It can also refer to the APIs that apps use to protect files and Keychain items.
Device Firmware Upgrade (DFU)	A mode in which a device's Boot ROM code waits to be recovered over USB. The screen is black when in DFU mode, but upon connecting to a computer running iTunes, the following prompt is presented: "iTunes has detected an iPad in recovery mode. You must restore this iPad before it can be used with iTunes."
ECID	A 64-bit identifier that's unique to the processor in each iOS device. When a call is answered on one device, ringing of nearby iCloud-paired devices is terminated by briefly advertising via Bluetooth Low Energy 4.0. The advertising bytes are encrypted using the same method as Handoff advertisements. Used as part of the personalization process, it's not considered a secret.
Effaceable Storage	A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely. While it doesn't provide protection if an attacker has physical possession of a device, keys held in Effaceable Storage can be used as part of a key hierarchy to facilitate fast wipe and forward security.
File system key	The key that encrypts each file's metadata, including its class key. This is kept in Effaceable Storage to facilitate fast wipe, rather than confidentiality.
Group ID (GID)	Like the UID but common to every processor in a class.
Hardware security module (HSM)	A specialized tamper-resistant computer that safeguards and manages digital keys.
iBoot	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
Identity Service (IDS)	Apple's directory of iMessage public keys, APNs addresses, and phone numbers and email addresses that are used to look up the keys and device addresses.
Integrated circuit (IC)	Also known as a microchip.
Joint Test Action Group (JTAG)	Standard hardware debugging tool used by programmers and circuit developers.

Keybag	A data structure used to store a collection of class keys. Each type (user, device, system, backup, escrow, or iCloud Backup) has the same format: • A header containing: – Version (set to three in iOS 5) – Type (system, backup, escrow, or iCloud Backup) – Keybag UUID – An HMAC if the keybag is signed – The method used for wrapping the class keys: tangling with the UID or PBKDF2, along with the salt and iteration count • A list of class keys: – Key UUID – Class (which file or Keychain Data Protection class this is) – Wrapping type (UID-derived key only; UID-derived key and – passcode-derived key) – Wrapped class key – Public key for asymmetric classes
Keychain	The infrastructure and a set of APIs used by iOS and third-party apps to store and retrieve passwords, keys, and other sensitive credentials.
Key wrapping	Encrypting one key with another. iOS uses NIST AES key wrapping, as per RFC 3394.
Low-Level Bootloader (LLB)	Code that's invoked by the Boot ROM, and in turn loads iBoot, as part of the secure boot chain.
Per-file key	The AES 256-bit key used to encrypt a file on the file system. The per-file key is wrapped by a class key and is stored in the file's metadata.
Provisioning Profile	A plist signed by Apple that contains a set of entities and entitlements allowing apps to be installed and tested on an iOS device. A development Provisioning Profile lists the devices that a developer has chosen for ad hoc distribution, and a distribution Provisioning Profile contains the app ID of an enterprise-developed app.
Ridge flow angle mapping	A mathematical representation of the direction and width of the ridges extracted from a portion of a fingerprint.
Smart card	An integrated, embedded circuit that provides secure identification, authentication, and data storage.
System on a chip (SoC)	An integrated circuit (IC) that incorporates multiple components into a single chip. The Secure Enclave is an SoC within Apple's A7 or later central processors.
Tangling	An integrated circuit (IC) that incorporates multiple components into a single chip. The Secure Enclave is an SoC within Apple's A7 or later central processors. The process by which a user's passcode is turned into a cryptographic key and strengthened with the device's UID. This ensures that a brute-force attack must be performed on a given device, and thus is rate limited and can't be performed in parallel. The tangling algorithm is PBKDF2, which uses AES keyed with the device UID as the pseudorandom function (PRF) for each iteration.
Uniform Resource Identifier (URI)	A string of characters that identifies a web-based resource.
Unique ID (UID)	A 256-bit AES key that's burned into each processor at manufacture. It can't be read by firmware or software, and is used only by the processor's hardware AES engine. To obtain the actual key, an attacker would have to mount a highly sophisticated and expensive physical attack against the processor's silicon. The UID isn't related to any other identifier on the device including, but not limited to, the UDID.
XNU	The kernel at the heart of the iOS and macOS operating systems. It's assumed to be trusted, and enforces security measures such as code signing, sandboxing, entitlement checking, and ASLR.

Document Revision History

Date	Summary
January 2018	**Updated for iOS 11.2** • Apple Pay Cash **Updated for iOS 11.1** • Security Certifications and Programs • Touch ID/Face ID • Shared Notes • CloudKit end-to-end encryption • TLS • Apple Pay, Paying with Apple Pay on the web • Siri Suggestions • Shared iPad • For more information about the security contents of iOS 11 go to: https://support.apple.com/HT208112
July 2017	**Updated for iOS 10.3** • System Enclave • File Data Protection • Keybags • Security Certifications and programs • SiriKit • HealthKit • Network Security • Bluetooth • Shared iPad • Lost Mode • Activation Lock • Privacy Controls • For more information about the security contents of iOS 10.3 go to: https://support.apple.com/HT207617
March 2017	**Updated for iOS 10** • System Security • Data protection classes • Security Certifications and programs • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Single Sign-on • Apple Pay, Paying with Apple Pay on the web • Credit, debit, and prepaid card provisioning • Safari Suggestions • For more information about the security contents of iOS 10 go to: https://support.apple.com/HT207143

Date	Summary
May 2016	**Updated for iOS 9.3** • Managed Apple ID • Two-factor authentication for Apple ID • Keybags • Security Certifications • Lost Mode, Activation Lock • Secure Notes • Apple School Manager, Shared iPad • For more information about the security contents of iOS 9.3 go to: https://support.apple.com/HT206166
September 2015	**Updated for iOS 9** • Apple Watch Activation Lock • Passcode policies • Touch ID API support • Data Protection on A8 uses AES-XTS • Keybags for unattended software update • Certification updates • Enterprise app trust model • Data protection for Safari bookmarks • App Transport Security • VPN specifications • iCloud Remote Access for HomeKit • Apple Pay Rewards cards, Apple Pay card issuer's app • Spotlight on-device indexing • iOS Pairing Model • Apple Configurator 2 • Restrictions • For more information about the security contents of iOS 9 go to: https://support.apple.com/HT205212

January 2018

(b) (4)

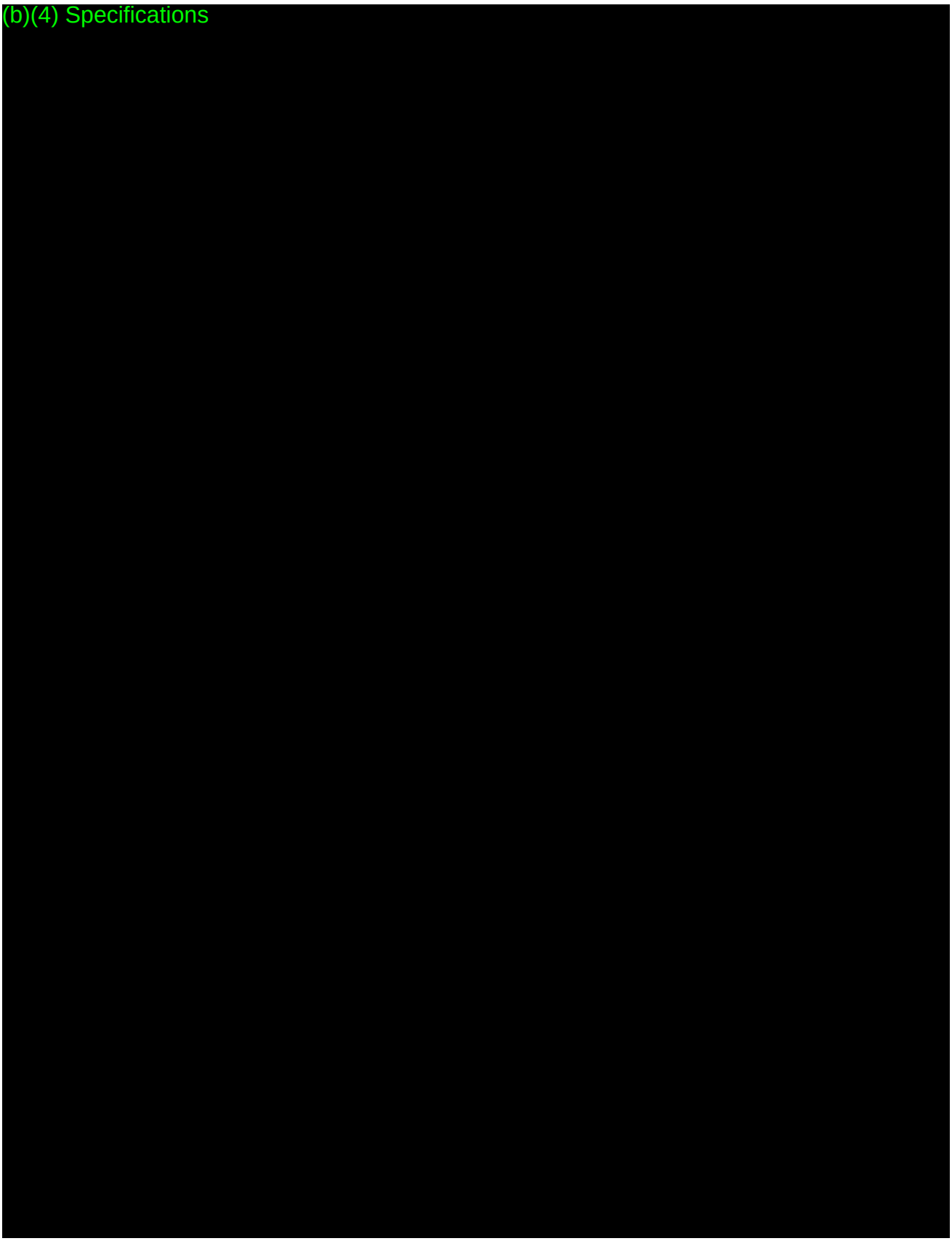
(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Draft

(b)(4) Specifications



(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Appendix O
Verification (QA) Testing Report

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

(b)(4) Copyrighted Materials

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Tuesday, August 28, 2018 7:04 PM
To: Gremi, Erdit; Ricci, Linda J; Paulsen, Jessica; Cruz, Marisa
Cc: Drummond, Arielle
Subject: AHS participant (b) (6)

FDA Team:

Below please find a written summary of the information we shared on the call today regarding the death of participant (b) (6) Please let me know if you need anything else.

All SAEs occurred on (b) (6) The dates referenced in your email are dates the event was received/created by (b) (6) It does not reflect the actual event onset date, but rather the date the case was generated by the Safety Desk. The Safety Desk created a placeholder for "unexplained death" because they did not have the official cause of death and could not assume other SAEs caused this patient's death.

(b) (6)

The participant did not receive any AF alert notifications during his participation in the study, and we have nothing to suggest that the participant or his wife relied on the app to make (or not make) any medical decisions.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Tuesday, August 28, 2018 9:14 AM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>

Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

External (erdit.gremi@fda.hhs.gov)

Report This Email Powered by Inky

Donna-Bea,

Can we get more information on (b) (6) ? The SAEs for this subject include:

(b) (6)
Chest pain
Could not breath
Unconscious
Unexplained death

Is there a reason why this patient did not appear to seek medical treatment despite having SAEs 3-4 days prior to the unexplained death while using the device? Did the watch provide any AF alert notifications during the time of the SAEs?

Eri Gremi

WO66 Room:1102
Tel: 240-402-3910

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Monday, August 27, 2018 8:27 PM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Attached please find the second item that was due today: Additional Information from the AHS study.

The final item for today will be sent directly to you by my client.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 6:17 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; 'Paulsen, Jessica' <Jessica.Paulsen@fda.hhs.gov>; 'Cruz, Marisa' <Marisa.Cruz@fda.hhs.gov>; 'Gremi, Erdit' <Erdit.Gremi@fda.hhs.gov>
Cc: 'Drummond, Arielle' <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA team:

Attached please find the first of the items due today: Additional information for (b) (4) Intended Use population (Aug. 23 email).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 1:18 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Here is the updated status on outstanding items:

Items to be provided by end of today (August 27)
- Responses to (b) (4) questions (Aug. 22 email)
- Additional information in (b) (4) Intended Use population (Aug. 23 email)
- Additional data from AHS study

Items to be provide by end of the day tomorrow (August 28)
- Responses to (b) Clinical/Performance questions (August 24 email)
- (b) Validation for the platform input to the app

In regards to (b) (4) Validation for the platform input to the app, we will let you know by the end of the day today when we expect to have that information.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Monday, August 27, 2018 11:55 AM
To: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: interactive review

Hello Donna-Bea,

We would like to see where we are with the requests for:

- Validation data for the input to each of the apps (b) (4)
- Timing for responses to outstanding issues
- Timing for AHS data request

Please either provide an update via email before 1 or we can discuss at 1. If you can provide by email, then we are comfortable cancelling the 1pm call.

Thanks!
--Linda

Linda Ricci
Associate Director ODE DH

Center for Devices and Radiologic Health
Office of Device Evaluation
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

Excellent customer service is important to us. Please take a moment to provide feedback regarding the customer service you have received: https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Wednesday, August 22, 2018 8:32 PM
To: Gremi, Erdit; Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle
Subject: (b) (4) Alert level sensitivity and specificity

We are providing the following additional information in response to FDA's request for alert level sensitivity and specificity.

(b) (4)

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Thursday, August 30, 2018 9:22 PM
To: Ricci, Linda J; Paulsen, Jessica; Gremi, Erdit; Drummond, Arielle
Subject: (b) (4) additional information
Attachments: (b) (4) Responses 20180830.pdf

FDA Team:

Here are our responses to what we believe to be all of the remaining (b) (4) questions, with the exception of: 1) the recent FDA email on changes to the IFU and 2) the results of final "platform validation testing" (to be submitted Sept. 4).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Wednesday, August 22, 2018 9:44 PM
To: Gremi, Erdit; Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle
Subject: (b) (4) design mitigation
Attachments: PastedGraphic-5.pdf

FDA Team:

Attached please find a proposed design change (b) (4)

The key changes are as follows:
(b) (4)

Our team will be available to discuss these changes with you during the 1pm phone call Thursday.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Gremi, Erdit

From: Gremi, Erdit
Sent: Thursday, August 30, 2018 3:19 PM
To: Donna-Bea Tillman; 'Calley Herzog'
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: (b) (4) IFU revisions

Donna-Bea,

We have identified some additional IFU revisions that we want to propose for (b) (4) Please let us know if you concur with the changes.

(b)(4) Draft

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Saturday, August 18, 2018 10:55 AM
To: Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle; Gremi, Erdit
Subject: (b) (4) Interactive review request information
Attachments: (b) Summary for Skin Tone Aug 17.pdf; FDA Interactive Review Open Items_20180818.xlsx; Follow-up to (b) (4) CV Data Call_Aug 14 .pdf; HF FDA Questions Aug 16.pdf

FDA Team:

Attached please find the following items for (b) (4)

1. Responses to the questions raised by FDA during the August 14 call on the (b) (4) CV study
2. A summary of the (b) study that responds to FDA's questions regarding what data we have regarding (b) (4) performance with different skin tones
3. Our response to the first two of the three human factors questions you sent on August 16. We are still discussing your third question regarding additional mitigations and will provide a response next week.

I have also provided an updated spreadsheet that is tracking the open items that we have received so far. Please let me know if we have missed anything

Have a good weekend, and we will talk to you on Monday.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Skin Tone Evaluation From Large-Scale Live-On Study

1. Objective

The purpose of this study was to do engineering validation on (b) (4) algorithm performance. This study report summarized the results of skin tone analysis of the study subjects.

2. Study Population

Summary inclusion criteria: 50-85 years old, able to read and understand consent and follow study procedures.

Summary exclusion criteria: pregnancy, pacemaker or ICD, active skin disorder or open wound(s) on forearm, wrist tattoos, inability to safely participate in study.

Skin Tone Distribution: the study aimed to recruit at least N=50 subjects with Fitzpatrick VI skin.

3. Impact on Algorithms

(b) (4)

(b) (4)

4. Protocol

The study was administered at multiple sites across the US. Study subjects participated for up to 4 days and contributed data both day and night.

Skin tone was assessed at intake. Fitzpatrick skin type was graded visually by comparing to a reference scale. Skin lightness (L*) was measured with a spectrophotometer at the point on the wrist where the Watch was worn.

(b) (4)

After the study interval was complete the subject returned to the study site to remove the ECG electrodes and return study equipment for data download and transmission back to Apple.

Collected data were analyzed with the platform and (b) (4) algorithms offline.

5. Results

(b) (4)

(b) (4)

6. Impact of Skin Tone

Because of the high absorptivity of melanin at the green wavelength used by the platform sensor, dark skin tone is expected to result in smaller signal amplitude and hence has the potential to make PPG heart rate measurements more difficult. In order to address the full consumer population, the platform sensor was designed to produce adequate signal levels across the full range of human skin tone. The platform sensor is able to increase the LED current (and hence light output), photodiode gain (sensitivity to light), and sampling rate to ensure the raw PPG signal is in a range with adequate SNR; (b) (4)

To ensure robust end-to-end performance of this feature, the (b) (4) population was intentionally biased to have greater representation of very dark skin than is expected from the general US population. The distribution of skin tone in the (b) (4) study population is shown in Figures 1 and 2. Nearly 5% of subjects had Fitz VI skin (and nearly 9% had L* < 40). According to the 2010 US Census, 12.6% of the US population

is of African descent [1]. A recent study of Fitzpatrick skin types reported that only 15% of Africans can be classified as having Fitzpatrick VI skin. This suggests that it has prevalence of only about 2% in the US population [2].

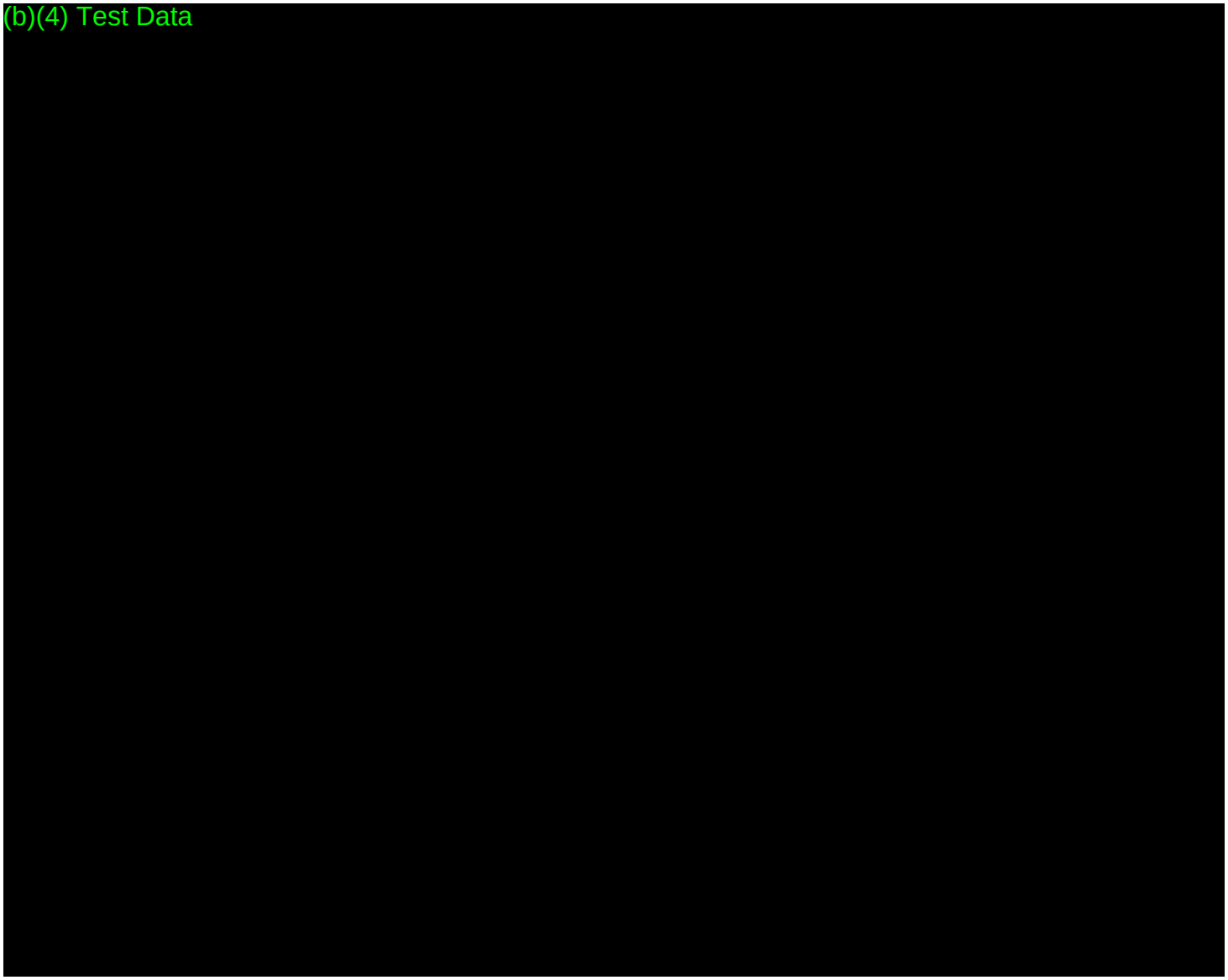
(b) (4)

[redacted]

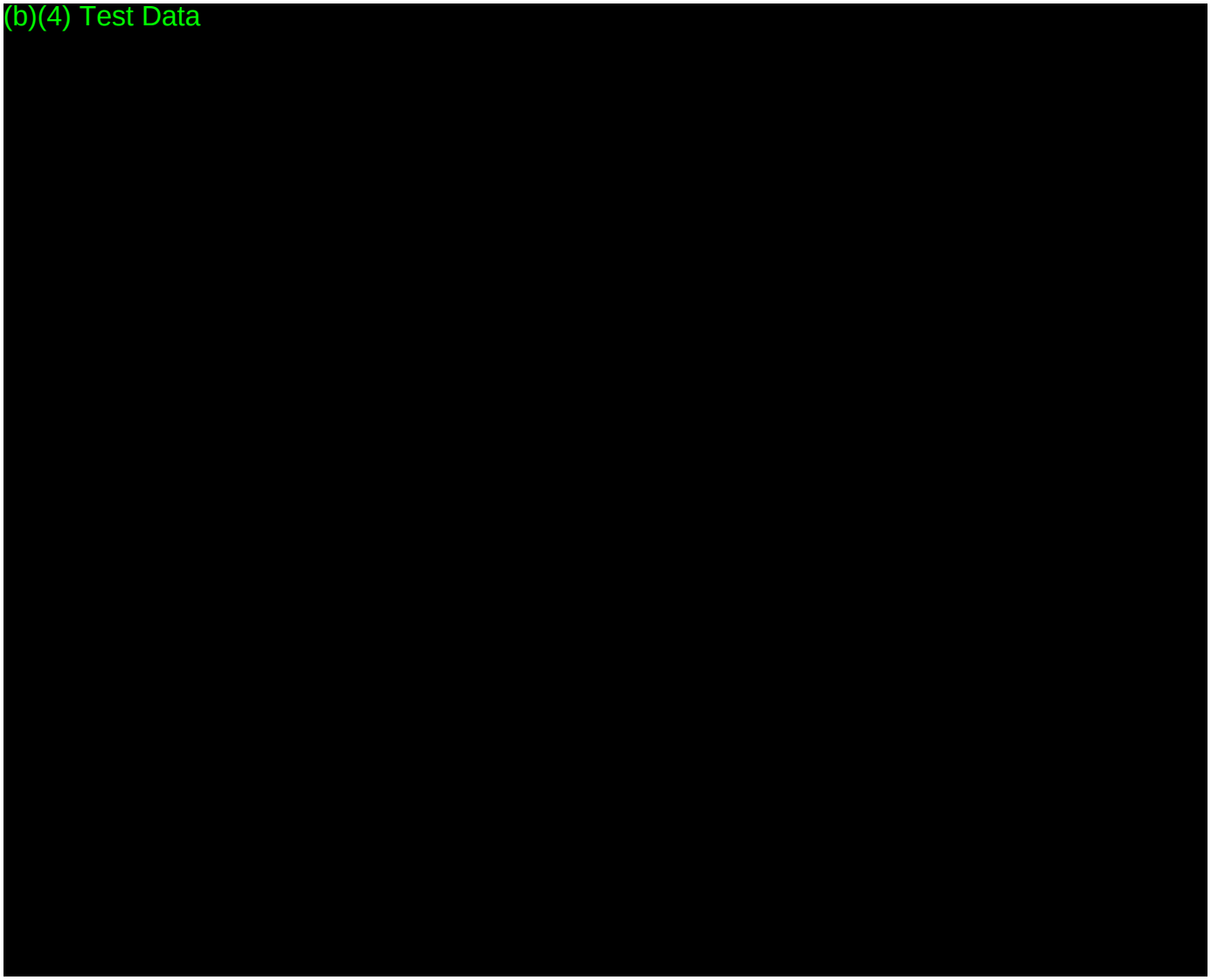
7. References

[1] US Census 2010, available online: https://www2.census.gov/geo/maps/dc10_thematic/2010_Profile/2010_Profile_Map_United_States.pdf

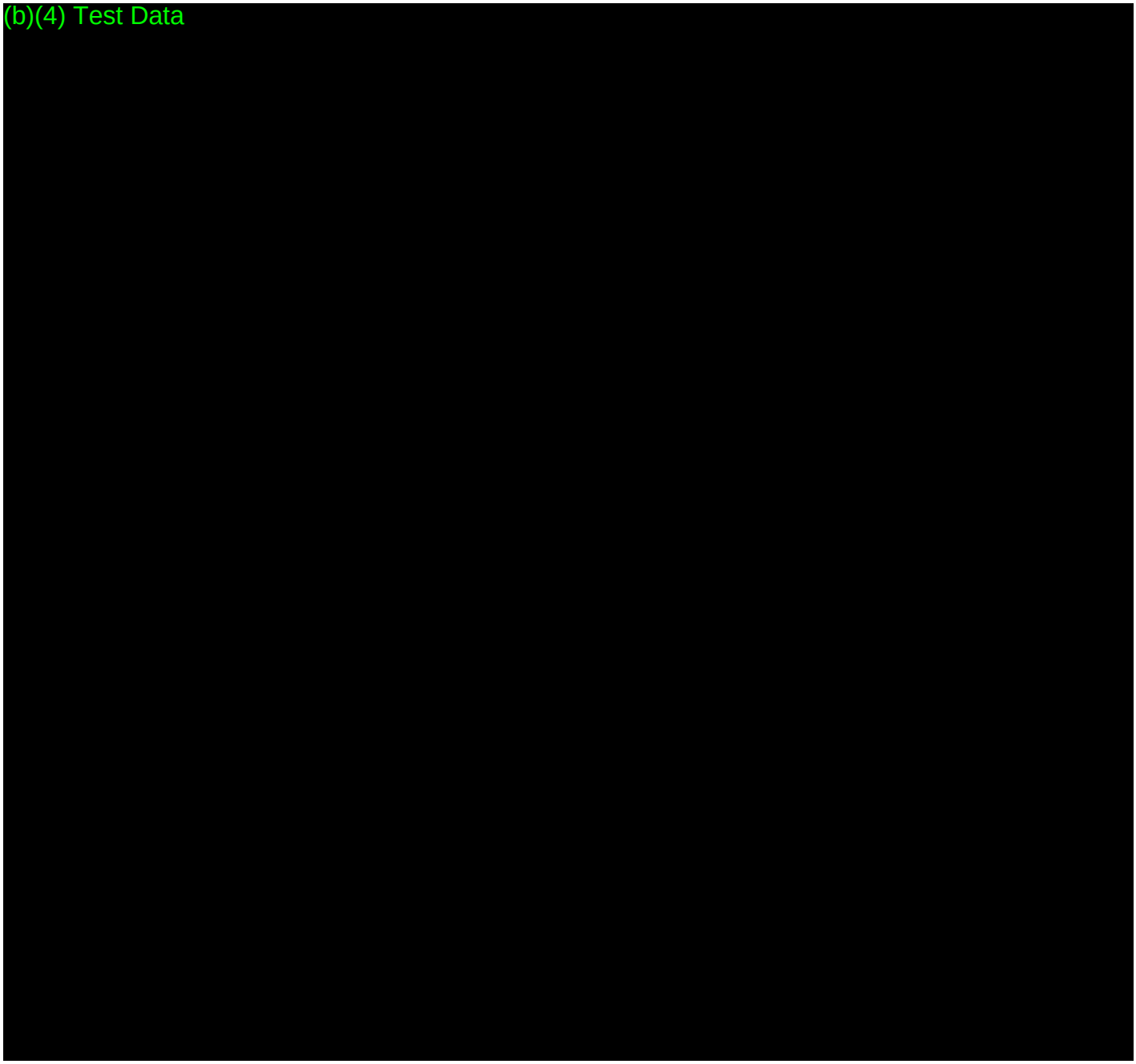
[2] Eilers S. et al., "Accuracy of self-report in assessing Fitzpatrick skin phototypes I through VI," JAMA Dermatol., 2013, pp 1289-94.



(b)(4) Test Data



(b)(4) Test Data



(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Wednesday, August 29, 2018 10:40 PM
To: Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle; Gremi, Erdit
Subject: (b) (4) Platform Inputs Testing
Attachments: Aug 29 (b) (4) Platform Test Coverage.pdf

FDA Team:

Attached please find the (b) (4) Platform Inputs testing for (b) (4) Note that (b) (4) is referred to in the reports as (b) (4)

As we have discussed, complete testing for (b) (4) will be provided on September 4.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Tuesday, September 4, 2018 8:17 PM
To: Ricci, Linda J; Gremi, Erdit; Paulsen, Jessica; Drummond, Arielle
Subject: (b) (4) Platform Testing
Attachments: (b) (4) Platform Test Coverage and Report 04SEP2018.pdf

FDA Team:

Attached please find the (b) (4) platform testing for Watch (b) (4) Let me know if you have any questions.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Tuesday, August 21, 2018 9:44 PM
To: Ricci, Linda J; Drummond, Arielle; Paulsen, Jessica; Gremi, Erdit
Subject: (b) (4) responses and Tracker
Attachments: FDA Interactive Review Tracker.xlsx; (b) (4) Responses 8.21.2018.pdf

FDA team:

Attached please find our responses for the Interactive review questions posed by FDA for (b) (4) through August 19 (see the Tracker for details). We will be providing responses to the (b) (4) questions received 8/21 by the end of the day Thursday (8/23).

Regards,

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Lewis, LaToye

From: Gremi, Erdit
Sent: Wednesday, August 29, 2018 3:54 PM
To: 'Donna-Bea Tillman'; Calley Herzog
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: Clarifying question

Donna Bea,

(b) (4)

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Thursday, August 9, 2018 4:43 PM
To: Gremi, Erdit
Cc: Paulsen, Jessica; Drummond, Arielle; Ricci, Linda J; Calley Herzog
Subject: DEN180042 - Clinical Study Report
Attachments: AHS_Substudy_Clinical Study Report_FINAL.pdf

Erdit:

Attached please find a .pdf of the (b) (4) App document "Appendix E Clinical Study report". The eCopy de novo supplement will arrive at FDA on Monday at the latest (possibly Friday) and will include all report appendices and listings as well as the raw data and statistics files.

We look forward to walking you through the study design and results, and to answering any of your questions during the WebEx currently scheduled for next Tuesday at 11:30am.

Please don't hesitate to reach out to Calley or me if you need anything.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Calley Herzog <cherzog@biologicsconsulting.com>
Sent: Wednesday, August 8, 2018 2:45 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Hi Erdit,

I am confirming that the documents on the ecopy that will be delivered to the DCC tomorrow are the exact same documents you have been provided by email today and yesterday. They are not revisions intended to replace any of those emailed documents.

The only additional items that will be on the ecopy, but were not provided by email yesterday and today are:

- **Appendix D** (b) (4) **Human Factors Summative Study Report:** This file was too large to email. It will be included in the complete ecopy
- **References:** These were not provided by email but will be included in the complete ecopy
- **Cover Letter:** (attached). It provides explanation of the ecopy content.

Kind Regards,
Calley

Please note: I will be out of the office Aug 17 - 23
Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct
cherzog@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Wednesday, August 8, 2018 12:33 PM
To: Calley Herzog <cherzog@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Calley,

Thank you for the quick turn around and the additional documents. I just want to confirm with you; are the additional documents that will be submitted through DCC going to revise any of the documents that have been included in these emails or will they simply be additional information and detail?

Eri Gremi

WO66 Room:1102
Tel: 240-402-3910

From: Calley Herzog [mailto:cherzog@biologicsconsulting.com]
Sent: Wednesday, August 8, 2018 1:36 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Erdit,

Attached is a zip file containing the redlined version of the de novo main body as well as the remaining Appendices with the exception of the following:

- **Appendix E Clinical Study report:** This will be provided as a supplement to the de novo. We will email the clinical study report on Friday. Ecopy will arrive at FDA on Monday and will include all report appendices and listings as well as the raw data and statistics files.
- **Appendix D** (b) (4) **Human Factors Summative Study Report:** This file is too large to email. It will be included in the complete ecopy to be delivered to the DCC tomorrow.
- **References:** These will be included in the complete ecopy to be delivered to the DCC tomorrow.

Please confirm receipt. I am not sure if the attachment is too large. If so, I can break it into multiple emails.

Kind Regards,
Calley

Please note: I will be out of the office Aug 17 - 23
Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct
cherzog@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Wednesday, August 8, 2018 7:51 AM
To: Calley Herzog <cherzog@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Calley,

After a cursory review of the email contents you provided there seem to be some documents missing that we had expected to be in the submission. The missing documents are:

- Revised hazards analysis
- Software Testing (V&V)
- Traceability Analysis
- Unresolved Anomalies
- Revision level history
- OTS (Off the Shelf Software) documentation

I recognize that the email you provided may not necessarily be an exhaustive list of documents that are arriving in the official submission. However, we will need these documents for the substantive review of the (b) (4) app. Please let me know if you have any questions and when we can expect to have these documents for review.

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Calley Herzog [mailto:cherzog@biologicsconsulting.com]
Sent: Tuesday, August 7, 2018 3:41 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: (b) (4) - de novo documents

Erdit,

As promised, I am providing the following (b) (4) documents as attachments to this email:

- De novo main body
- Appendix I – SRS (both clean and redlined)
- Appendix J – SDS
- Appendix P – responses to FDA Questions

These documents, along with all remaining appendices except for the clinical study report will be delivered to FDA as a de novo submission on Thursday (8/9). The clinical study report will be provided by email on Friday (8/10), followed by an ecopy delivered to FDA on Monday (8/13) as a supplement to the de novo.

Please let us know if you have any questions or concerns about the timeline or submission process.

Kind Regards,
Calley

Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct
cherzog@biologicsconsulting.com
BiologicsConsulting.com

APPLE HEART STUDY SUB-STUDY

Clinical Study Report

August 7, 2018

Apple Inc.

This study was conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, clinical research guidelines established by the U.S. Food and Drug Administration (21 CFR Parts 50, 54, 56, and 812), and ICH GCP Guidelines.

TABLE OF CONTENTS

TABLES

LISTINGS

APPENDICES

1. LIST OF ABBREVIATIONS AND DEFINITIONS OF TERMS

The following abbreviations and specialist terms are used in this study report.

Abbreviation or Specialist Term	Explanation
ADE	Adverse Device Effect
AF	Atrial Fibrillation/Atrial Flutter
AHS	Apple Heart Study
AT	Atrial Tachycardia
CFR	Code of Federal Regulations
CRO	Clinical Research Organization
EAS	ECG Analysis Set
ECG	Electrocardiogram
FAS	Full Analysis Set
FDA	Food and Drug Administration
GCP	Good Clinical Practice
H_0	Null Hypothesis
H_A	Alternative Hypothesis
HRV	Heart Rate Variability
ICF	Informed Consent Form
ICH	International Conference on Harmonization
IRB	Institutional Review Board
J-Beat	Junctional Beats
SA	Sinus Arrhythmia
SAP	Statistical Analysis Plan
SR	Sinus Rhythm
PAC	Premature Atrial Contractions
PPG	Photoplethysmogram
PPV	Positive Predictive Value
PVC	Premature Ventricular Contractions
QC	Quality Control
VF	Ventricular Fibrillation
VT	Ventricular Tachycardia

2. PROTOCOL SYNOPSIS

Overview

This Apple Heart Study Sub-Study (AHS Sub-Study) Protocol describes the analysis that will be conducted on a subset of data from the ongoing Apple Heart Study. This AHS Sub-Study is being conducted to determine if the tachogram classification algorithm and confirmation cycle algorithm (alert-level) have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF) in a subset of AHS participants.

Study Objective

The objective of this AHS Sub-Study is to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable positive predictive value (PPV) as compared to ambulatory electrocardiographic (ECG) patch monitoring in identifying irregular rhythms consistent with atrial fibrillation (AF).

Study Endpoints

1. Primary Endpoint: Identification of irregular rhythm consistent with AF as suggested by positive predictive value (PPV) of the spot tachogram (Spot Tachogram PPV)
2. Secondary Endpoint: Identification of irregular rhythm consistent with AF as suggested by PPV of the notification (Alert-Level PPV)
3. Primary Safety Endpoint: Serious adverse device effects (ADEs)

Study Hypothesis

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b)

H_0: $PPV_{Tachogram(AF)}$ (b)

vs.

H_A: $PPV_{Tachogram(AF)}$ (b)

There are no hypotheses specified for the secondary endpoint or the safety endpoint.

Subject Population

AHS began on November 30, 2017. The data to support this sub-study will come from AHS participants who were enrolled between November 30, 2017, to June 22, 2018, who have received the ECG patch (ePatch provided by BioTelemetry) and for whom ECG data has been adjudicated. The analysis defined in this sub-study protocol will not be initiated until all participant data (up to June 22, 2018) to be used in the analysis is available.

To ensure the confidentiality of the subject data, subject data will be identified by a participant ID number for which the Sponsor will not have the ability to link back to the subject's identity. The

use of the data in this sub-study is consistent with the disclosure of research aims and use of the data made to the subjects in the IRB-approved Apple Heart Study informed consent form.

The inclusion/exclusion criteria for the AHS is as follows:

Inclusion Criteria

Subjects must meet all the following inclusion criteria to be enrolled:

1. Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:
   I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.
   II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.
2. Age ≥ 22 years at time of eligibility screening, ascertained from self-reported date of birth.
3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.
4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.
5. Valid phone number associated with iPhone, ascertained from self-report.
6. Valid email address, ascertained from self-report.

Exclusion Criteria

Subjects who meet any of the following criteria may not be enrolled:

1. Self-reported diagnosis of Atrial Fibrillation at time of consent.
2. Self-reported diagnosis of Atrial Flutter at time of consent.
3. Currently on anticoagulation therapy, as self-reported at the time of consent.

Sample Size

The sample size in this sub-study is the number of spot tachograms. (b) (4) [redacted]

3. ETHICS

3.1. Institutional Review Board

Using the Department of Health and Human Services regulations found at 45 CFR 46.101(b)(4), the Institutional Review Board (IRB) determined that the Apple Heart Study (AHS) Sub-Study is exempt from IRB oversight. Documentation of IRB-exempt status was obtained. Details of the IRB are provided in Appendix B.

3.2. Ethical Conduct of the Study

The AHS Sub-Study was designed and monitored in accordance with Sponsor procedures, which comply with the ethical principles of Good Clinical Practice (GCP) as required by the major regulatory authorities, and in accordance with the Declaration of Helsinki.

3.3. Informed Consent

Informed consent was obtained from all AHS participants from whom data is being used to support data analysis for the AHS Sub-Study. Study participants were informed that their study data could be used in the context of a regulatory submission and for commercial purposes. No additional informed consent for this sub-study was required.

Informed Consent Process in the Apple Heart Study (AHS)

The AHS is an ongoing app-based research study being conducted through the AHS app. As in other mobile-mediated research studies, the informed consent process in the AHS was conducted remotely in a completely self-administered setting with no required contact with the research team prior to consent and enrollment.

The potential participant first downloaded the AHS app. The app automatically ensured compatibility with the iPhone iOS version and Watch version. If compatible, the participant was able to continue forward in the app. An overview of the study was also displayed in the app.

The participant then advanced to a screen for study enrollment, where he/she confirmed whether general participation requirements were met. The participant was asked questions based on study inclusion and exclusion criteria. The app automatically determined eligibility based on the responses provided. If the participant was determined to be eligible, he/she was presented with an in-app consent and authorization form to be read and signed if the participant agreed to participate.

A copy of the signed study consent and authorization document was available for review and download to the participant via the app. After consenting to participate, the participant was directed to complete a brief questionnaire to collect self-reported baseline demographics and medical history. The participant was considered ‘enrolled’ from this point and the study app’s analysis of Apple Watch Photoplethysmogram (PPG) sensor data began thereafter.

The approach to informed consent for the AHS was meant to ensure that participants were adequately informed about the research before agreeing to participate. Potential candidates as well

as enrolled participants were able to contact an AHS hotline (available 24/7 at 1-844-606-1609) any time and had the ability to ask questions, request clarifications, or report a problem at any time prior to or during the study. This hotline was opened from the study start date and will remain open until study closure.

4. INVESTIGATORS AND STUDY ADMINISTRATIVE STRUCTURE

4.1. Investigators

Investigative sites were not utilized during this sub-study. This clinical study report (CSR) includes data from subjects who were enrolled between November 30, 2017, and June 22, 2018, who received an ePatch and for whom ECG data was adjudicated in the AHS, an app-based research study conducted in the United States.

4.2. Study Administrative Structure

4.2.1. Sponsor Responsibilities

The AHS Sub-study is an analysis on a pre-specified subset of data collected in the AHS to support a regulatory submission before the AHS ends. AHS is an app-based research non-significant risk study and was sponsored by Apple Inc. The Sponsor developed the protocol and statistical analysis plan (SAP) to conduct this sub-study.

The Sponsor's responsible Clinical/Regulatory Study Representative attested to the accuracy of this report and his/her signature is provided in Appendix A.

The Sponsor recruited and managed the contract research organizations (CROs).

4.2.2. Contract Research Organization (CRO) Responsibilities

Three independent ECG adjudicators (BioTelemetry, Inc., Malvern, PA) provided review and adjudication of ECG strips with oversight by the Sponsor.

The adjudicators were required to have U.S. board-certification in Cardiology and/or Electrophysiology, with extensive and relevant experience in clinical, clinical research, and/or event adjudication expertise as assessed by review of their CVs.

5. INTRODUCTION

5.1. Background

Atrial fibrillation (AF) is the most common serious cardiac arrhythmia, and, when left untreated, is a leading cause of morbidity and mortality from stroke, heart failure and myocardial infarction[1,2]. Data from the Framingham Heart Study indicates that by age 40 years, lifetime risk for developing AF is 1 in 4. AF is also a growing public health problem with prevalence projected to triple between 2010 and 2050, with an estimated 12.1 million diagnosed cases in 2030 in the United States alone.

Early detection and treatment of patients with AF minimizes the risk of sequelae of thromboembolism including >60% reduced risk of stroke[2]. However, many affected with AF are unaware they have this arrhythmia due to a number of factors, including lack of symptoms, or they may experience only mild symptoms that they do not attribute to a disease[2]. As a result, asymptomatic patients are 3 times as likely to have sustained an ischemic stroke prior to diagnosis than those with symptoms[1]. These findings raise concerns and have prompted several variations of screening programs to detect patients with asymptomatic AF to prevent an embolic event[1,2]. While systematic and opportunistic screening programs have demonstrated increased rates of detection when compared to detection during routine clinical practice, such screening programs are not yet widely implemented[2]. Additionally, AF may be paroxysmal (PAF, or intermittent AF) and therefore missed by recording a single in-clinic electrocardiogram (ECG). This is especially true for those patients with intermittent symptoms. Holter devices are commonly used for ambulatory 24-hour ECG monitoring in at-risk patients but have limited sensitivity for the detection of new AF[7].

5.2. Device Description and Purpose of the Sub-Study

This sub-study used data collected from a subset of participants enrolled in the *Apple Heart Study: Assessment of Wristwatch-Based Photoplethysmography to Identify Cardiac Arrhythmias*, which is a large, prospective, single arm, experimental non-significant risk study, conducted with the assistance of eligible participants without a known history of atrial fibrillation or atrial flutter (at the time of consent). The subjects in this sub-study received an irregular rhythm notification within the AHS App and consequently received and wore an ambulatory ECG patch (ePatch) for interpretation of the ambulatory ECG findings by trained ECG technicians.

The AHS app is a mobile medical application used in the ongoing AHS. Because the AHS study is being conducted completely virtually, the app functions as a means to screen for inclusion/exclusion criteria, collect the electronic informed consent, collect user information and medical history, and is used by the subjects to connect to a Study Telehealth Provider if they receive an irregular rhythm notification or if they need to report a problem (described in section above). The app also contains the tachogram classification algorithm and alert-level confirmation cycle algorithm, both of which were validated in this sub-study.

The tachogram classification algorithm classified a tachogram as irregular or not AF, and the alert-level confirmation cycle algorithm determined if a notification was surfaced to the user. At baseline, the Apple Watch platform attempted to capture a tachogram every 2-4 hours to support

the commercially available heart rate variability (HRV) feature, and the AHS app retrieved and analyzed any such tachograms that were captured. If a tachogram was classified as irregular, the "confirmation cycle" began, during which the AHS app requested additional tachograms from the platform more frequently (as frequently as possible, subject to a minimum spacing of 15 minutes). If five out of six sequential tachograms (including the initial one) were classified as irregular within a 48-hour period, a notification of this finding was surfaced to the user. If two tachograms were classified as not AF before this threshold was reached, the AHS app returned to baseline (attempting to retrieve tachograms every 2-4 hours), no results were surfaced, and the confirmation cycle was reset (that is, any irregular tachograms within this sequence did not count in future confirmation cycles).

When the AHS app surfaced the first notification to the user, the workflow to call the Study Telehealth Provider and receive the ambulatory ECG monitor (ePatch) was initiated. After the first notification was surfaced, no additional notifications were surfaced to the user. However, notifications continued to be generated for the purposes of data analysis ("silent notifications"). The classified tachograms that contributed to a notification and the notification itself were stored and used for the alert-level positive predictive value (PPV) analysis.

The tachogram and notification data collected and processed through the algorithms within the AHS app are the subject of this sub-study and were compared to the gold-standard ECG (ePatch) to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV. The data analyzed in this sub-study was obtained from AHS participants who were enrolled between November 30, 2017, and June 22, 2018, who received an ePatch and for whom ECG data was adjudicated. The AHS Sub-study analysis was conducted prior to the completion of the AHS.

6. STUDY OBJECTIVE

The objective of this AHS Sub-Study was to determine if the tachogram classification algorithm and alert-level confirmation cycle algorithm have acceptable PPV as compared to the ePatch monitoring in identifying irregular rhythms consistent with AF.

7. STUDY ENDPOINTS

7.1. Primary Efficacy Endpoint

The primary efficacy endpoint of this sub-study is the identification of irregular rhythm consistent with AF as suggested by PPV of the spot tachogram where the ePatch readings (paired to the timestamp associated with the spot tachograms) were used for the determination of AF. Each subject may have contributed multiple observations (i.e., spot tachograms) for this endpoint.

7.2. Secondary Efficacy Endpoint

The secondary efficacy endpoint is the identification of irregular rhythm consistent with AF as suggested by PPV of the alert (based on multiple irregular tachograms) where the ePatch readings were used for the determination of AF. Each subject may have contributed no more than one observation to the analysis of this endpoint.

7.3. Additional Analyses

- Spot tachogram PPV for AF and other arrhythmias
- Alert-level PPV for AF and other arrhythmias
- Sensitivity for AF and specificity for SR for spot tachograms

7.4. Primary Safety Endpoint

The primary safety endpoint is the incidence of serious adverse device effects (ADEs). Adverse device effects are being collected in the ongoing AHS. All serious ADEs reported by participants whose data are included in this sub-study and adjudicated on or before June 22, 2018, were summarized in this CSR.

8. STUDY HYPOTHESIS

The primary efficacy endpoint study hypothesis is that the tachogram-level PPV for AF is at least (b)

H_0: $PPV_{Tachogram\ (AF)}$ (b)

vs.

H_A: $PPV_{Tachogram\ (AF)}$ (b)

There are no hypotheses specified for the secondary efficacy endpoint, additional analyses, or the primary safety endpoint.

9. INVESTIGATIONAL PLAN

9.1. Overall Study Design and Plan

This sub-study used data collected from a subset of participants enrolled in the *Apple Heart Study: Assessment of Wristwatch-Based Photoplethysmography to Identify Cardiac Arrhythmias*, which is a large, prospective, single arm, experimental non-significant risk study, conducted with the assistance of eligible participants without a known history of atrial fibrillation or atrial flutter (at the time of consent). The subjects in this sub-study received an irregular rhythm notification within the AHS App and consequently received and wore an ambulatory ECG patch (ePatch) for interpretation of the ambulatory ECG findings by trained ECG technicians.

All study data were coded with a participant identification (ID). Additional consent was not required to be obtained for this sub-study as this study was determined to be exempt from IRB oversight. The use of the data in this sub-study is consistent with the disclosure of research aims and use of data made to participants in the IRB-approved AHS informed consent.

No additional participation requirements or data, outside of those already required in AHS, were requested of the participants for the purposes of this sub-study analysis.

9.1.1. Study Data Collection Procedures

AHS Study Procedures

Participants in AHS wear their Apple Watch as per normal usage with the AHS App's algorithms analyzing collected PPG pulse data, with two possible outcomes:

1. No irregular heart rhythms consistent with AF that meet the notification threshold are identified from the time monitoring begins (after consenting)

   or;

2. Irregular heart rhythms consistent with AF are identified that meet notification threshold (complete confirmation cycle) during the study. The participant is then notified via the app of this irregularity. Participants who receive a notification during the study will enter the positive notification workflow.

Positive Notification Workflow

The app notification will provide a button for the participant to connect with the Study Telehealth Provider. Upon successful connection, the participant is asked about cardiovascular clinical signs and symptoms. If the Study Telehealth Provider concludes that the participant has a medical emergency, the Study Telehealth Provider will follow its emergency protocol and either instruct the participant and/or a family member, if available, to call emergency medical services (EMS) or will call on the participant's behalf if the participant and/or a family member are unable to contact EMS. These participants will not receive the ambulatory ECG monitors.

Otherwise, if eligible to receive the ePatch, the Study Telehealth Provider will provide the participant information about the ePatch, answer any questions the participant might have, and contact BioTelemetry to initiate the order and shipment of the ePatch.

The BioTelemetry ePatch Monitor will be used for ambulatory ECG monitoring. The battery life with a single channel recording is 7 days. The participant will be instructed to wear the ePatch for up to 7 days. However, the data collected from a participant will be considered adequate for a participant with a minimum analyzable time of 1 hour.

Data Collection and Processing

1. In AHS, eligible participants are sent an ePatch, instructed to wear the patch for up to seven days, and mail the ePatch back to BioTelemetry for processing. BioTelemetry processes the ECG data and generates a standard report for the purposes of the AHS. BioTelemetry also sends raw ECG data to the Sponsor securely for storage. A subset of this data was used for the purposes of this sub-study.

(b) (4)

[redacted]

Data Review

Analysis of ePatch ECG Strips

Two primary, independent adjudicators reviewed each complete ECG strip and provided a diagnosis of the rhythm. The adjudicators classified each of the ECG strips. If there were any differences in the adjudication decisions, the strip in question was sent to a third adjudicator for final decision.

(b) (4)

2. The diagnosis of the rhythm fell into one of four categories:

    i. Sinus Rhythm (SR)
    ii. Atrial Fibrillation (AF)*
    iii. Other Irregular Rhythm (defined below)
    iv. Unreadable (a diagnosis cannot be made as the strip is not adequate for reading)

    *While atrial fibrillation and atrial flutter are two separate conditions, they often manifest similarly in the ECG and can be difficult to differentiate. Clinical treatment of the two conditions is the same. Therefore, for the purposes of this study, the conditions are considered the same.

3. The diagnosis was made via the following logic flow (in sequential order):

(b) (4)

Algorithm Classification

a) The tachogram classification algorithm generated a rhythm classification for a given tachogram, which fell into one of two categories:

   i. Irregular
   ii. Not AF

(b) (4)

The ECG adjudicators were blinded to the tachogram rhythm classifications.

An ECG Adjudication Charter was developed with details of the ECG adjudication process as well as adjudicator qualification criteria and used for adjudicator training purposes.

9.2. Study Population

9.2.1. Inclusion and Exclusion Criteria

In AHS, subjects were required to meet all the following inclusion criteria to be enrolled:

1. Possession of the following at time of eligibility screening, ascertained from automatic hardware/software/device pairing check:
   I. iPhone (5s or later) with iOS version 11.0 or later defined as iPhone model/iOS version used to complete screening eligibility.
   II. Apple Watch (Series 1 or later) with watchOS version 4.0 or later defined as Apple Watch model/watchOS paired with iPhone used to complete screening eligibility.
2. Age ≥ 22 years at time of eligibility screening, ascertained from self-reported date of birth.
3. Current resident of the United States at time of eligibility screening, defined by self-reported state of residence within the 50 states of the United States or District of Columbia.
4. Proficient in written and spoken English, defined by self-report of comfort reading, writing, and speaking English on iPhone.
5. Valid phone number associated with iPhone, ascertained from self-report.
6. Valid email address, ascertained from self-report.

In AHS, subjects who met any of the following criteria were excluded from enrollment:

1. Self-reported diagnosis of atrial fibrillation at time of consent.

2. Self-reported diagnosis of atrial flutter at time of consent.
3. Currently on anticoagulation therapy, as self-reported at the time of consent.

9.2.2. Removal of Subjects from the Study

The sub-study analysis was conducted on a pre-specified group of subjects from the larger AHS. No subjects were removed from the sub-study.

9.2.3. Randomization and Blinding

The design of this sub-study was not randomized.

Independent technologists with extensive and relevant experience reviewed and interpreted the ECG data obtained during the course of the parent AHS. For the purposes of this sub-study, two primary independent adjudicators received (b) strips that corresponded to tachogram time points collected by the Apple Watch. The adjudicators classified each of the ECG strips. If there were any differences in the adjudication decisions, the strip in question was sent to a third adjudicator for final decision.

For the primary endpoint, multiple spot tachograms were generated for each subject during the time of ECG patch wear. (b) (4)

9.3. Efficacy and Safety Variables

9.3.1. Subject, Spot Tachogram, Alert, and ECG Measurement Accountability

Summary tables which presents subject accountability and spot tachogram, alert, and ECG patch measurement result accountability are reported in **Table 1.1** and **Table 2.2**, respectively.

9.3.2. Demographic and Other Baseline Characteristics

Descriptive statistics (e.g., N, Mean, Std. Dev., Min, Max) for continuous data types and frequencies for categorical data types are displayed for the following demographic and other baseline characteristics in **Table 3**. The following age group categories were used: 22-39, 40-54, 55-64, and 65+:

- Age (Continuous and categorical)
- Sex (Categorical)
- Race (Categorical)
- Height (Continuous)

- Weight (Continuous)
- BMI (Continuous)
- CHA2DS2-VASc score (Continuous)
- Medical History (Categorical)
- Number of cigarettes smoked per day (Categorical)
- Number of alcoholic beverages consumed per week (Categorical)

Subjects may have chosen more than one race category.

9.3.3. Adverse Events

Adverse events were collected through the AHS. All serious adverse device effects (ADEs) reported by participants whose data contributed to this sub-study and were adjudicated on or before June 22, 2018, were considered and analyzed for this sub-study.

9.3.4. Protocol Deviations

Protocol deviations were not captured as part of this sub-study.

9.4. Data Quality Assurance

There was no additional study monitoring for the purposes of the AHS Sub-Study. The data from AHS was monitored in accordance with ICH GCP guidelines.

The Sponsor or designee provided and maintained a charter that describes the independent review and training process for ECG reviewers.

The Sponsor or designee performed internal quality management of data collection, documentation and completion. Quality Control (QC) procedures were implemented beginning with the data entry system (ECG adjudication spreadsheet) and data QC checks that were incorporated into the database (ECG adjudication spreadsheet). Any missing data or data anomalies were communicated to the Sponsor for clarification and resolution.

9.5. Statistical Methods and Determination of Sample Size

9.5.1. Statistical and Analytical Plans

The statistical methods used for the analyses of data are described in the Statistical Analysis Plan (SAP) (Version 3.0, July 26, 2018), which is provided in **Appendix D**. All analyses were performed with SAS, v9.4 or higher and R (b) (4) in a Microsoft Windows environment.

9.5.1.1. Primary Endpoint Analyses

(b) (4) the primary efficacy endpoint of spot tachogram-level PPV for AF was estimated as follows:

$PPV_{Tachogram(AF)}$ = (# of spot tachograms classified as AF according to the spot tachogram algorithm and where the paired ECG strip is classified as AF) / (# of spot tachograms classified as AF according to the spot tachogram algorithm)

A one-sided 97.5% lower confidence bound was computed using an unadjusted normal distribution approximation to the binomial. If the lower bound for the spot tachogram-level PPV exceeded (b) the null hypothesis, H_0, would have been rejected.

(b) (4)

[redacted]

9.5.1.2. Secondary Endpoint Analyses

The alert-level PPV for AF was estimated as follows (b) (4)

[redacted]

$PPV_{Alert(AF)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF) / (# of alert notifications classified as AF according to the alert notification algorithm)

A two-sided exact 95% confidence interval was computed.

(b) (4)

[redacted]

9.5.1.3. Significance Level

The primary hypothesis test of the tachogram-level PPV used a one-sided significance level of 0.025. Two-sided 95% confidence intervals for the secondary and additional analyses are reported.

9.5.1.4. Missing Data/Outliers

Some planned measurements may not have been readable or obtainable. The data analyses were conducted on all readable/classifiable data. No outliers were removed from the analyses after investigation by the Sponsor.

9.5.1.5. Interim Analyses

There were no interim analyses planned in this sub-study.

9.5.1.6. Analysis Sets

All subjects in this sub-study received an AF notification and received an ePatch for ambulatory ECG monitoring. Two analysis sets were pre-defined for this sub-study.

Full Analysis Set (FAS): The Full Analysis Set (FAS) consists of subjects who received an ambulatory ECG monitor and wore their ePatch per the AHS protocol (i.e., were enrolled in this sub-study). Subject accountability, demographic, medical history, and adverse event information are presented for subjects in this analysis set.

ECG Analysis Set (EAS): (b) (4) [redacted] The identification of the subjects to be removed from the EAS were finalized prior to data analysis. All tachogram-level and alert-level outcomes were estimated from this analysis set during times when tachograms and alerts were recorded by Apple Watch during simultaneous, analyzable ECG monitoring.

9.5.1.7. Additional Analyses

For each of the additional endpoint analyses presented below, two-sided 95% confidence intervals are reported using an unadjusted normal distribution approximation to the binomial. A two-sided exact 95% confidence interval are reported for the alert-level PPV for AF and other arrhythmias.

9.5.1.7.1. Spot Tachogram PPV for AF and Other Arrhythmias

The spot tachogram PPV for AF and other arrhythmias were estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) [redacted]

$PPV_{Tachogram(AF\ and\ OA)}$ = (# of spot tachograms classified as AF according to the spot tachogram algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of spot tachograms classified as AF according to the spot tachogram algorithm)

9.5.1.7.2. Alert-Level PPV for AF and Other Arrhythmias

The alert-level (PPV) for AF and Other Arrhythmias were estimated as follows and reported along with its associated two-sided 95% confidence interval. (b) (4) [redacted] Each subject contributed only one alert notification in this analysis.

$PPV_{Alert\ (AF\ and\ OA)}$ = (# of alert notifications classified as AF according to the alert notification algorithm and where the paired ECG strip is classified as AF or Other Arrhythmia) / (# of alert notifications classified as AF according to the alert notification algorithm).

9.5.1.7.3. Spot Tachogram Sensitivity and Specificity

(b) (4) [redacted] the spot tachogram sensitivity (for AF) and specificity (for Sinus Rhythm) are calculated and reported along with the corresponding two-sided 95% confidence intervals.

(b) (4) [redacted]

9.5.2. Determination of Sample Size

The sample size for the primary endpoint of this sub-study is the number of spot tachograms indicating an irregular heart rhythm. (b) (4) [redacted]

9.6. Changes in the Conduct of the Study or Planned Analyses

The AHS Sub-Study Protocol (Version 2.0, June 22, 2018) is provided in Appendix C. There were no changes to the study conduct or planned analyses.

10. EFFICACY EVALUATION

10.1. Subject Accountability

Table 1.1 presents the subject accountability in the Full Analysis Set (FAS).

A total of 269 subjects were included in the FAS. Of the 269, 27 subjects were removed from the FAS due to data exclusions and 16 subjects were removed due to lack of ePatch data. Efficacy analyses were performed using the ECG analysis set (EAS) (subjects with ePatch data and tachogram data), which included 226 subjects. Refer to **Listing 8** for the list of subjects excluded from the efficacy analysis.

Table 1.1 Subject Accountability - Full Analysis Set

	Value
Subjects in FAS	269
Subjects Removed from FAS due to Data Exclusions	27
(b) (4) [redacted]	
Subjects in FAS with no Data Exclusions	242
Subjects with no ePatch or Tachogram Data	16
Subjects with ePatch Data and Tachogram Data	226
(b) (4) [redacted]	

10.2. Spot Tachogram, Alert, and ECG Measurement Accountability

Table 2.2 presents spot tachogram, alert, and ECG measurement accountability in the EAS, which included a total of 226 subjects.

The average number of spot tachograms contributed per subject was 46.3 tachograms.

Of the 10,432 total tachograms across all subjects, 25.4% (2650/10432) were classified as 'irregular' and 74.6% (7782/10432) were classified as 'Not AF' by the algorithm. All 10,432 tachograms were reviewed by two primary reviewers; (b) (4) [redacted]

Of the 226 subjects, 25.2% (57/226) received at least one alert during ePatch wear whereas 74.8% (169/226) of subjects did not receive any alert during ePatch wear.

Table 2.2 Spot Tachogram, Alert, and ECG Measurement Accountability - EAS

	Value
Number of Subjects in ECG Analysis Set	226
Spot Tachograms Per Subject	
Number of Subjects	226
(b) (4) [redacted]	
Spot Tachogram Classifications	
Irregular	2650 (25.4%)
Not AF	7782 (74.6%)
Total	10432 (100.0%)
(b) (4) [redacted]	

(b) (4)

10.3. Demographic and Other Baseline Characteristics

Table 3 presents demographics and other baseline characteristics for the FAS.

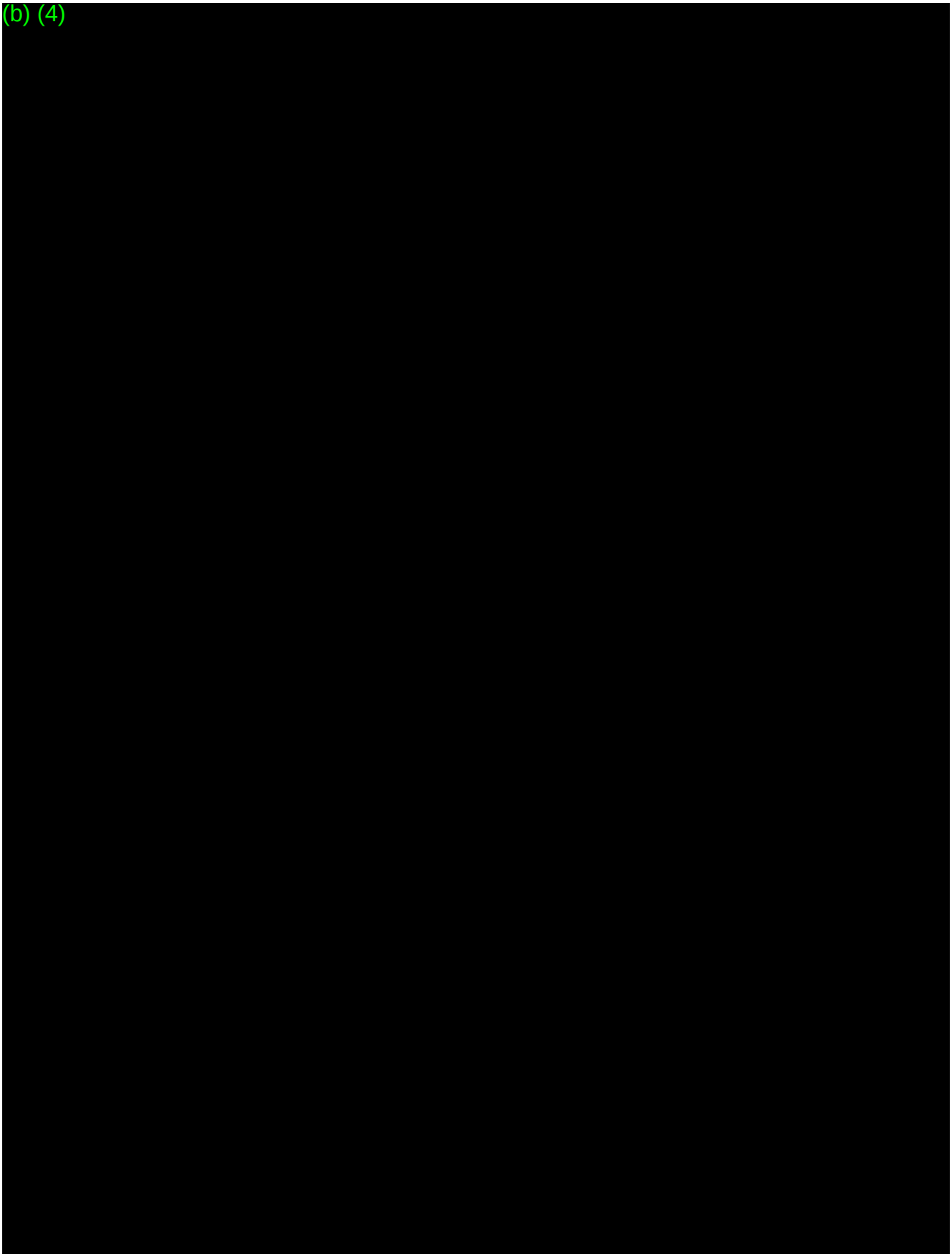
Overall, 80.2% (210/269) of subjects were Male, and 88.8% (239/269) of subjects were White. The mean age of subjects was 59.2 years. Refer to **Listing 2** for details of subject demographics and other baseline characteristics.

(b) (4) [redacted]

Table 3 Demographic and Other Baseline Characteristics – FAS

Characteristic	Subjects (N=269)
Age at Enrollment (years)	
N	268
Mean	59.2
(b) (4) [redacted]	
Age Group [N (%)]	
22-39	27 (10.1%)
40-54	58 (21.6%)
55-64	73 (27.2%)
65+	110 (41.0%)
Sex [N (%)]	
Male	210 (80.2%)
Female	52 (19.8%)
Other	0 (0.0%)
Unknown	0 (0.0%)
(b) (4) [redacted]	

(b) (4)



(b) (4)

10.4. Efficacy Results

10.4.1. Primary Efficacy Endpoint Analysis

Table 4 presents the primary endpoint analysis of spot tachogram PPV for the ECG Analysis Set.

(b) (4)

The spot tachogram PPV analysis resulted in a value of 66.6% (lower confidence bound = 63.0%, p-value 0.9841), which was lower than the pre-specified spot tachogram PPV (b) (4)

Refer to **Listing 4** for detailed ePatch adjudication results.

Table 4 Primary Endpoint Analysis of Spot Tachogram PPV - EAS

Parameter	Value	Lower Confidence Bound**	p-value***
(b) (4)			
Spot Tachogram PPV for AF	(b) (4) (66.6%)	63.0%	0.9841
(b) (4)			

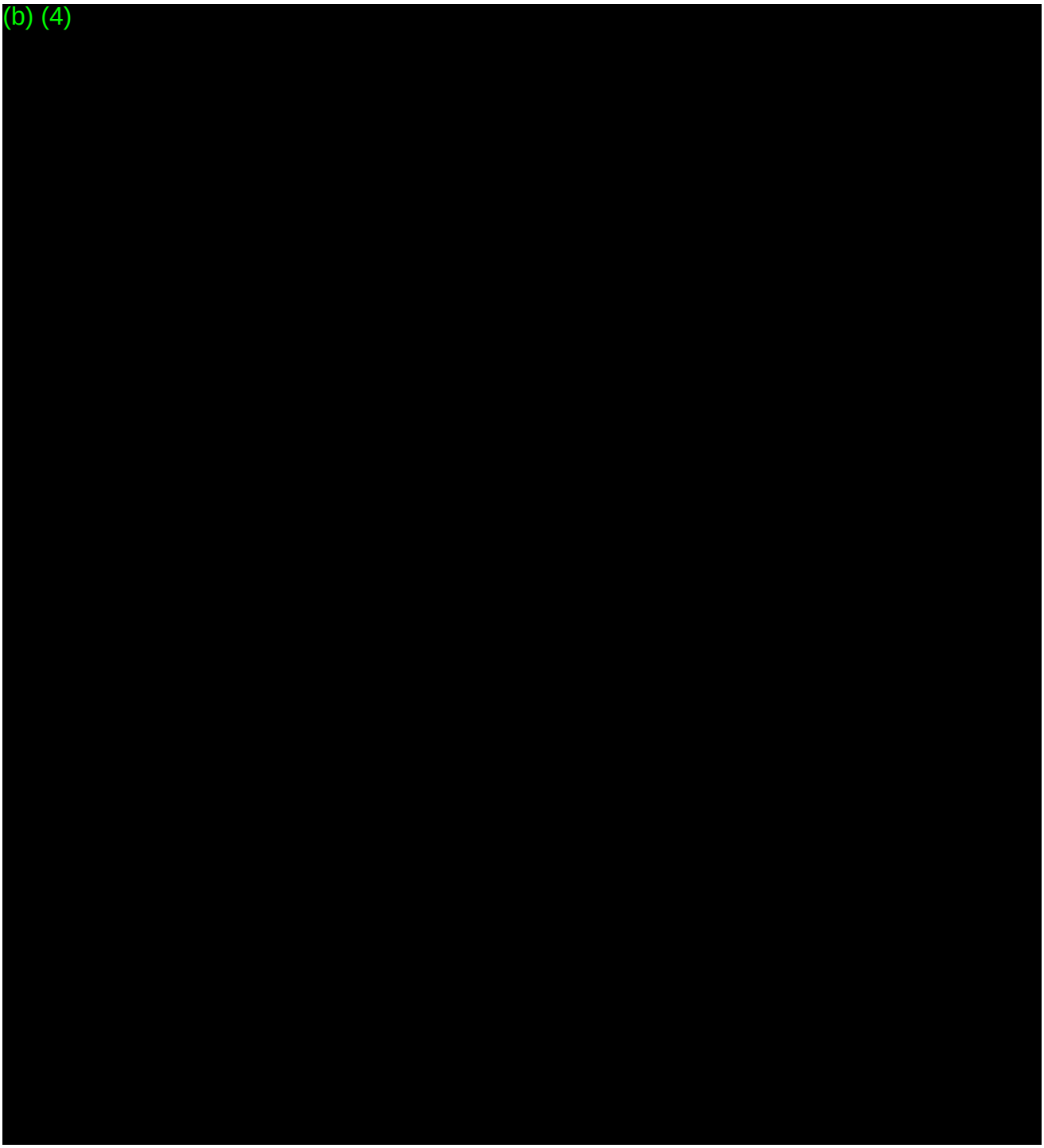
**Lower one-sided 97.5% confidence bound.

***Test of hypothesis for spot tachogram PPV (b)

10.4.2. Primary Efficacy Endpoint (b) (4)

(b) (4)

(b) (4)



(b) (4)

[redacted]

10.4.3. Secondary Efficacy Endpoint Analysis

Table 8 presents the secondary endpoint analysis of alert-level PPV for AF in the EAS.

There were 57 subjects with at least one alert-level notification. Of the 57 subjects who received an alert, 45 had at least one tachogram comprising the alert, which corresponded to an ePatch adjudicated result of AF.

The alert-level PPV for AF was 78.9% (45/57) with a two-sided 95% exact confidence interval of (66.1%, 88.6%).

There was no hypothesis associated with the secondary endpoint analysis.

Table 8 Secondary Endpoint Analysis of Alert-Level PPV for AF – EAS

Parameter	Value	Two-Sided 95% Exact Confidence Interval
Number of Subjects with at least 1 alert-level notification*	57	
Alert-level PPV for Atrial Fibrillation/Atrial Flutter	45/57 (78.9%)	(66.1%, 88.6%)
(b) (4) [redacted]		

Note: Numerator for PPV is the number of alerts where at least one of the ePatch results associated with the spot tachograms that comprise the alert is Atrial Fibrillation/Atrial Flutter.

10.4.4. Secondary Efficacy Endpoint Robustness Analyses

(b) (4)

[redacted]

(b) (4)

10.4.5. Additional Analyses

10.4.5.1. Spot Tachogram PPV for AF and Other Arrhythmias

Table 10 presents the spot tachogram PPV for AF and other arrhythmias in the EAS. There were 99 subjects who received at least one irregular tachogram, (b) (4) The analysis resulted in a spot tachogram PPV value of 98.4% (837/851) for AF and other arrhythmias.

Table 10 Additional Analysis: Spot Tachogram PPV for AF and Other Arrhythmias - EAS

Parameter	Value	Two-Sided 95% Confidence Interval
Number of subjects with at least 1 irregular spot tachogram	99	
(b) (4)		
	(b) (4)	(97.5%, 99.2%)
(b) (4)		

10.4.5.2. Alert-Level PPV for AF and Other Arrhythmias

Table 11 presents the alert-level PPV for AF and other arrhythmias in the EAS.

Across the 57 subjects with at least one alert during ePatch wear, the alert-level PPV for AF and other arrhythmias was 98.2% (56/57).

Table 11 Additional Analysis: Alert-Level PPV for AF and Other Arrhythmias – EAS

Parameter	Value	Two-Sided 95% Exact Confidence Interval
Number of Subjects with at least 1 alert-level notification*	57	
Alert-level PPV for AFib/Atrial Flutter and Other Arrythmias	56/57 (98.2%)	(90.6%, 100.0%)
(b) (4)		
*Irregular alert randomly selected from each subject if more than one available.		
Note: Numerator for PPV is the number of alerts where at least one of the ePatch results associated with the spot tachograms that comprise the alert is either Atrial Fibrillation or Other.		

10.4.5.3. Spot Tachogram Sensitivity and Specificity

Table 12 presents the spot tachogram sensitivity and specificity analysis conducted in the EAS.

The sensitivity was 82.9% (b) (4) with a lower confidence interval of 81.4%. The specificity was 99.8% (b) (4) with a lower confidence interval of 99.6%.

Table 12 Additional Analysis: Spot Tachogram Sensitivity and Specificity – EAS

Parameter	Value	Two-Sided Confidence Interval*
(b) (4)		
Sensitivity	(b) (4) (82.9%)	(81.4%, 84.4%)
(b) (4)		
Specificity	(b) (4) (99.8%)	(99.6%, 99.9%)
(b) (4)		

11. SAFETY EVALUATION

11.1. Primary Safety Endpoint Analysis

There were no device-related serious adverse device effects (SADEs) reported in the sub-study.

12. DISCUSSION AND OVERALL CONCLUSIONS

In this sub-study, there were 269 subjects included in the Full Analysis Set (FAS) and 226 subjects in the ECG Analysis Set (EAS). A summary of the results are as follows:

- The primary efficacy endpoint analysis for spot tachogram PPV (b) (4) resulted in a value of **66.6%** (lower confidence bound = 63.0%, p-value 0.9841). This fell below the pre-specified spot tachogram PPV (b) (4)

  (b) (4)

- The secondary efficacy endpoint of alert-level PPV is **78.9%** with a two-sided 95% exact confidence interval of (66.1%, 88.6%) (b) (4)

  (b) (4)

- Additional analyses were conducted with the following results:
  - Spot tachogram PPV for AF and other arrhythmias is **98.4%**.
  - Alert level PPV for AF and Other Arrhythmias is **98.2%**.
  - Spot tachogram sensitivity for AF is **82.9%** and specificity for SR is **99.8%**.
- There were no serious adverse device effects.

13. REFERENCE LIST

[1] Ben Freedman S, Lowres N. Asymptomatic Atrial Fibrillation: The Case for Screening to Prevent Stroke. JAMA. 2015 Nov 10;314(18):1911-2. doi: 10.1001/jama.2015.9846.

[2] Moran PS1, Teljeur C, Ryan M, Smith SM. Systematic screening for the detection of atrial fibrillation. Cochrane Database Syst Rev. 2016 Jun 3;(6):CD009586. doi: 10.1002/14651858.CD009586.pub3.

[3] Lloyd-Jones DM1, Wang TJ, Leip EP, Larson MG, Levy D, Vasan RS, D'Agostino RB, Massaro JM, Beiser A, Wolf PA, Benjamin EJ. Lifetime risk for development of atrial fibrillation: the Framingham Heart Study. Circulation. 2004 Aug 31;110(9):1042-6. Epub 2004 Aug 16.

[4] Colilla S1, Crow A, Petkun W, Singer DE, Simon T, Liu X. Estimates of current and future incidence and prevalence of atrial fibrillation in the U.S. adult population. Am J Cardiol. 2013 Oct 15;112(8):1142-7. doi: 10.1016/j.amjcard.2013.05.063. Epub 2013 Jul 4.

[5] Omboni S1, Verberk WJ2. Opportunistic screening of atrial fibrillation by automatic blood pressure measurement in the community. BMJ Open. 2016 Apr 12;6(4):e010745. doi: 10.1136/bmjopen-2015-010745.

[6] O'Neal WT1, Efird JT2, Judd SE3, McClure LA4, Howard VJ5, Howard G3, Soliman EZ6,7. Impact of Awareness and Patterns of Nonhospitalized Atrial Fibrillation on the Risk of Mortality: The Reasons for Geographic And Racial Differences in Stroke (REGARDS) Study. Clin Cardiol. 2016 Feb;39(2):103-10. doi: 10.1002/clc.22501. Epub 2016 Feb 16.

[7] Brachmann J1, Morillo CA2, Sanna T2, Di Lazzaro V2, Diener HC2, Bernstein RA2, Rymer M2, Ziegler PD2, Liu S2, Passman RS2. Uncovering Atrial Fibrillation Beyond Short-Term Monitoring in Cryptogenic Stroke Patients: Three-Year Results From the Cryptogenic Stroke and Underlying Atrial Fibrillation Trial. Circ Arrhythm Electrophysiol. 2016 Jan;9(1):e003333. doi: 10.1161/CIRCEP.115.003333.

[8] Evaluation and Reporting of Age-, Race-, and Ethnicity-Specific Data in Medical Device Clinical Studies. FDA Guidance Document. September 12, 2017.

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Tuesday, September 4, 2018 5:01 PM
To: Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle; Gremi, Erdit
Subject: DEN180042 ([redacted] Indications

FDA Team:

Attached are the updated proposed Indications for Use for the [redacted] DEN180042). Please let me know as soon as possible if you would like any additional changes.

[redacted]

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Calley,

I wanted to send over some issues that we have identified during the Human Factors review that we were hoping you might be able to provide some additional information on.

(b) (4)

[redacted]

(b) (4)

[redacted]

Thank you,
Erdit Gremi
Lead Reviewer
CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov<mailto:Erdit.Gremi@fda.hhs.gov>
[cid:image001.png@01D1C57E.DFA022A0]<http://www.fda.gov/>

[cid:image002.jpg@01D1C57E.DFA022A0]<https://www.facebook.com/FDA>
[cid:image003.jpg@01D1C57E.DFA022A0] <https://twitter.com/US_FDA>
[cid:image004.jpg@01D1C57E.DFA022A0]
<http://www.youtube.com/user/USFoodandDrugAdmin>
[cid:image005.jpg@01D1C57E.DFA022A0]
<http://www.flickr.com/photos/fdaphotos/>
[cid:image006.jpg@01D1C57E.DFA022A0]
<http://www.fda.gov/AboutFDA/ContactFDA/StayInformed/RSSFeeds/default.htm>

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Gremi, Erdit

From: Gremi, Erdit
Sent: Friday, August 17, 2018 1:10 PM
To: 'Donna-Bea Tillman'; 'Calley Herzog'
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: DEN180042 Clinical performance questions

Donna Bea,

I wanted to send over some issues that we have identified during the Clinical review that we were hoping you might be able to provide some additional information on by tomorrow (8/18/2018):

(b) (4)

(b) (4)

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Donna-Bea,

I wanted to send over some changes for the IFU which are necessary to better represent the device's intended use and align it more closely with the demonstrated performance in the clinical study. Please note that this may not be an exhaustive list of revisions necessary to make to the labeling documentation of the device, but it is what we have identified so far:

(b) (4)

[redacted]

Please let me know if you have any additional questions.

Erdit Gremi
Lead Reviewer
CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov<mailto:Erdit.Gremi@fda.hhs.gov>
[cid:image001.png@01D1C57E.DFA022A0]<http://www.fda.gov/>

[cid:image005.jpg@01D1C57E.DFA022A0]
<http://www.flickr.com/photos/fdaphotos/>
[cid:image006.jpg@01D1C57E.DFA022A0]
<http://www.fda.gov/AboutFDA/ContactFDA/StayInformed/RSSFeeds/default.htm
>

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service
you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Gremi, Erdit
Sent: Thursday, August 23, 2018 11:45 AM
To: 'Donna-Bea Tillman'; Calley Herzog
Cc: Paulsen, Jessica; Ricci, Linda J
Subject: DEN180042 Intended use population

Donna Bea,

(b) (4)

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Gremi, Erdit

From: Gremi, Erdit
Sent: Thursday, August 23, 2018 11:45 AM
To: 'Donna-Bea Tillman'; Calley Herzog
Cc: Paulsen, Jessica; Ricci, Linda J
Subject: DEN180042 Intended use population

Donna Bea,

(b) (4)

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Thursday, August 30, 2018 8:30 PM
To: Gremi, Erdit; Paulsen, Jessica; Ricci, Linda J; Drummond, Arielle
Subject: FW: (b) (4) IFU revisions

FDA Team:

(b) (4)

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Begin forwarded message:

From: "Gremi, Erdit" <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) **IFU revisions**
Date: August 30, 2018 at 3:19:21 PM EDT
To: Donna-Bea Tillman <donnabea@apple.com>, Calley Herzog <calley_herzog@apple.com>
Cc: "Ricci, Linda J" <Linda.Ricci@fda.hhs.gov>, "Paulsen, Jessica" <Jessica.Paulsen@fda.hhs.gov>

Donna-Bea,

We have identified some additional IFU revisions that we want to propose for (b) (4)
Please let us know if you concur with the changes.

(b) (4)

(b) (4)

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

=

Lewis, LaToye

From: donnabea@apple.com on behalf of Donna-Bea Tillman <donnabea@apple.com>
Sent: Thursday, August 30, 2018 5:12 PM
To: Gremi, Erdit
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: Re: (b) (4) IFU revisions

In the future, please send all email to my Biologics Consulting email address and not this one. I do not regularly monitor this email address.
dtillman@biologicsconsulting.com

Thanks!!

Donna-Bea Tillman
donnabea@apple.com

On Aug 30, 2018, at 5:10 PM, Donna-Bea Tillman <donnabea@apple.com> wrote:

Donna-Bea Tillman
donnabea@apple.com

On Aug 30, 2018, at 3:19 PM, Gremi, Erdit <Erdit.Gremi@fda.hhs.gov> wrote:

Donna-Bea,

We have identified some additional IFU revisions that we want to propose for (b) (4) Please let us know if you concur with the changes.

(b) (4)

(b) (4)

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov
<image001.png>

<image002.png> <image003.png> <image004.png> <image005.png> <image006.png>

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: donnabea@apple.com on behalf of Donna-Bea Tillman <donnabea@apple.com>
Sent: Thursday, August 30, 2018 5:10 PM
To: Gremi, Erdit
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: Re: (b) (4) IFU revisions

Donna-Bea Tillman
donnabea@apple.com

On Aug 30, 2018, at 3:19 PM, Gremi, Erdit <Erdit.Gremi@fda.hhs.gov> wrote:

Donna-Bea,

We have identified some additional IFU revisions that we want to propose for (b) (4)
Please let us know if you concur with the changes.

(b) (4)

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov
<image001.png>

<image002.png> <image003.png> <image004.png> <image005.png> <image006.png>

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Friday, August 31, 2018 8:21 AM
To: Ricci, Linda J; Gremi, Erdit; Paulsen, Jessica; Drummond, Arielle
Subject: RE: (b) (4) IFU revisions

FDA Team:

We agree to the proposed changes to the Indications for Use. Please let us know if there will be any other changes to the labeling. If not, we will send you a revised version of the labelling and an updated Form 3881 Indications for Use.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Thursday, August 30, 2018 8:45 PM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: (b) (4) IFU revisions

Yes, that is correct

Linda Ricci
Associate Director ODE DH

Office of Device Evaluation
Center for Devices and Radiologic Health
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Thursday, August 30, 2018 8:30 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: FW: (b) (4) IFU revisions

FDA Team:

(b) (4)

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Begin forwarded message:

From: "Gremi, Erdit" <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) **IFU revisions**
Date: August 30, 2018 at 3:19:21 PM EDT
To: Donna-Bea Tillman <donnabea@apple.com>, Calley Herzog <calley_herzog@apple.com>
Cc: "Ricci, Linda J" <Linda.Ricci@fda.hhs.gov>, "Paulsen, Jessica" <Jessica.Paulsen@fda.hhs.gov>

Donna-Bea,

We have identified some additional IFU revisions that we want to propose for (b) (4) Please let us know if you concur with the changes.

(b) (4)

(b) (4)

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

=

Gremi, Erdit

From: Gremi, Erdit
Sent: Saturday, August 18, 2018 4:26 PM
To: 'Donna-Bea Tillman'; Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle
Subject: RE: (b) (4) Interactive review request information

Donna-Bea,

It appears that the Interactive Review Open items does not include the items that were included in last night's email regarding the statistical and algorithm concerns. Just wanted to confirm with you if that was intentional or if there is a more recent version of the spreadsheet.

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Saturday, August 18, 2018 10:55 AM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) Interactive review request information

FDA Team:

Attached please find the following items for (b) (4)

1. Responses to the questions raised by FDA during the August 14 call on the (b) (4) CV study
2. A summary of the (b) study that responds to FDA's questions regarding what data we have regarding (b) (4) performance with different skin tones
3. Our response to the first two of the three human factors questions you sent on August 16. We are still discussing your third question regarding additional mitigations and will provide a response next week.

I have also provided an updated spreadsheet that is tracking the open items that we have received so far. Please let me know if we have missed anything

Have a good weekend, and we will talk to you on Monday.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Lewis, LaToye

From: Gremi, Erdit
Sent: Saturday, August 18, 2018 5:49 PM
To: 'Donna-Bea Tillman'; Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle
Subject: RE: (b) (4) Interactive review request information

Donna-Bea,

(b) (4)

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Saturday, August 18, 2018 4:46 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: (b) (4) Interactive review request information

Erdit:

We have definitely received that email and are already discussing it. I have added it to the spreadsheet (see attached).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Saturday, August 18, 2018 4:26 PM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: (b) (4) Interactive review request information

Donna-Bea,

It appears that the Interactive Review Open items does not include the items that were included in last night's email regarding the statistical and algorithm concerns. Just wanted to confirm with you if that was intentional or if there is a more recent version of the spreadsheet.

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Saturday, August 18, 2018 10:55 AM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle

<Arielle.Drummond@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) Interactive review request information

FDA Team:

Attached please find the following items for (b) (4)

1. Responses to the questions raised by FDA during the August 14 call on the (b) (4) CV study
2. A summary of the (b) study that responds to FDA's questions regarding what data we have regarding (b) (4) performance with different skin tones
3. Our response to the first two of the three human factors questions you sent on August 16. We are still discussing your third question regarding additional mitigations and will provide a response next week.

I have also provided an updated spreadsheet that is tracking the open items that we have received so far. Please let me know if we have missed anything

Have a good weekend, and we will talk to you on Monday.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Saturday, August 18, 2018 4:46 PM
To: Gremi, Erdit; Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle
Subject: RE: (b) (4) Interactive review request information
Attachments: FDA Interactive Review Open Items_20180818.xlsx

Erdit:

We have definitely received that email and are already discussing it. I have added it to the spreadsheet (see attached).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Saturday, August 18, 2018 4:26 PM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: (b) (4) Interactive review request information

Donna-Bea,

It appears that the Interactive Review Open items does not include the items that were included in last night's email regarding the statistical and algorithm concerns. Just wanted to confirm with you if that was intentional or if there is a more recent version of the spreadsheet.

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch

U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Saturday, August 18, 2018 10:55 AM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) Interactive review request information

FDA Team:

Attached please find the following items for (b) (4)

1. Responses to the questions raised by FDA during the August 14 call on the (b) (4) CV study
2. A summary of the (b) study that responds to FDA's questions regarding what data we have regarding (b) (4) performance with different skin tones
3. Our response to the first two of the three human factors questions you sent on August 16. We are still discussing your third question regarding additional mitigations and will provide a response next week.

I have also provided an updated spreadsheet that is tracking the open items that we have received so far. Please let me know if we have missed anything

Have a good weekend, and we will talk to you on Monday.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Gremi, Erdit

From: Gremi, Erdit
Sent: Wednesday, August 22, 2018 12:14 PM
To: 'Donna-Bea Tillman'; Ricci, Linda J; Drummond, Arielle; Paulsen, Jessica
Subject: RE: (b) (4) responses and Tracker

Donna-Bea,

For some of the statistical questions the response references that there is a revised R-code in a .zip file and data used to compute the confidence intervals using the (b) (4), but I couldn't find the zip file. Please send that over so we can take a look at the updated information.

Thanks,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Tuesday, August 21, 2018 9:44 PM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Subject: (b) (4) responses and Tracker

FDA team:

Attached please find our responses for the Interactive review questions posed by FDA for (b) (4) through August 19 (see the Tracker for details). We will be providing responses to the (b) (4) questions received 8/21 by the end of the day Thursday (8/23).

Regards,

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

Gremi, Erdit

From: Gremi, Erdit
Sent: Wednesday, August 29, 2018 4:51 PM
To: 'Donna-Bea Tillman'; 'Calley Herzog'
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: RE: Clarifying question

Donna Bea,

(b) (4)

[redacted]

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Gremi, Erdit
Sent: Wednesday, August 29, 2018 3:54 PM
To: 'Donna-Bea Tillman' <dtillman@biologicsconsulting.com>; Calley Herzog <calley_herzog@apple.com>
Cc: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>
Subject: Clarifying question

Donna Bea,

(b) (4)

[redacted]

(b) (4)

[redacted]

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Thursday, August 16, 2018 8:15 PM
To: Gremi, Erdit
Cc: Paulsen, Jessica; Ricci, Linda J; Calley Herzog
Subject: RE: Clinical Walkthrough Slides
Attachments: (b) (4) CV Study Overview for FDA.PDF; (b) (4) Clinical Data Review Aug 14 2018 - Meeting Minutes for FDA.PDF

Erdit:

Attached please find the slides from the (b) (4) clinical walkthrough and the minutes. Please let me know if you have any further questions.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Thursday, August 16, 2018 5:28 PM
To: Calley Herzog <cherzog@biologicsconsulting.com>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: Clinical Walkthrough Slides

Donna Bea,

Would you be able to send over the slides that we went over on the clinical walkthrough on Tuesday?

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

(b) (4)

(b) (4)

(b) (4)

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Thursday, August 9, 2018 5:38 PM
To: Gremi, Erdit
Cc: Paulsen, Jessica; Drummond, Arielle; Ricci, Linda J; Calley Herzog
Subject: RE: DEN180042 - Clinical Study Report

Erdit:

I received an acknowledgement email from the DMC at 3:30 today for the full de novo submission (see the document number on this email thread), so you should have the eCopy with everything except the clinical study report (which I emailed) and the clinical study report appendices (which will arrive Friday or Monday).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Thursday, August 9, 2018 5:33 PM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Calley Herzog <cherzog@biologicsconsulting.com>
Subject: RE: DEN180042 - Clinical Study Report

Donna-Bea,

Thank you for forwarding this to us ahead of the full de novo submission. I understand that the Appendix D (b) (4) Human Factors Summative Study Report was too large to email. However, waiting until possibly Monday is too long a delay for getting the Summative Report. If necessary, I am alright with receiving the file in multiple parts or via split zip files. I believe that our email file size limit is 20MB. Just include the email "1 of X" in the subject line and send them over so we can start the review. Please let me know if that plan works for you.

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman [mailto:dtillman@biologicsconsulting.com]
Sent: Thursday, August 9, 2018 4:43 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Calley Herzog <cherzog@biologicsconsulting.com>
Subject: DEN180042 - Clinical Study Report

Erdit:

Attached please find a .pdf of the (b) (4) App document “Appendix E Clinical Study report”. The eCopy de novo supplement will arrive at FDA on Monday at the latest (possibly Friday) and will include all report appendices and listings as well as the raw data and statistics files.

We look forward to walking you through the study design and results, and to answering any of your questions during the WebEx currently scheduled for next Tuesday at 11:30am.

Please don’t hesitate to reach out to Calley or me if you need anything.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Calley Herzog <cherzog@biologicsconsulting.com>
Sent: Wednesday, August 8, 2018 2:45 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Hi Erdit,

I am confirming that the documents on the ecopy that will be delivered to the DCC tomorrow are the exact same documents you have been provided by email today and yesterday. They are not revisions intended to replace any of those emailed documents.

The only additional items that will be on the ecopy, but were not provided by email yesterday and today are:

- **Appendix D** (b) (4) **Human Factors Summative Study Report:** This file was too large to email. It will be included in the complete ecopy
- **References:** These were not provided by email but will be included in the complete ecopy
- **Cover Letter:** (attached). It provides explanation of the ecopy content.

Kind Regards,
Calley

Please note: I will be out of the office Aug 17 - 23
Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct
cherzog@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Wednesday, August 8, 2018 12:33 PM
To: Calley Herzog <cherzog@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea

Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

External (erdit.gremi@fda.hhs.gov)

Report This Email Powered by Inky

Calley,

Thank you for the quick turn around and the additional documents. I just want to confirm with you; are the additional documents that will be submitted through DCC going to revise any of the documents that have been included in these emails or will they simply be additional information and detail?

Eri Gremi

WO66 Room:1102
Tel: 240-402-3910

Excellent customer service is important to us.
Please take a moment to provide feedback regarding the customer service you have received:
https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

From: Calley Herzog [mailto:cherzog@biologicsconsulting.com]
Sent: Wednesday, August 8, 2018 1:36 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Erdit,

Attached is a zip file containing the redlined version of the de novo main body as well as the remaining Appendices with the exception of the following:

- **Appendix E Clinical Study report:** This will be provided as a supplement to the de novo. We will email the clinical study report on Friday. Ecopy will arrive at FDA on Monday and will include all report appendices and listings as well as the raw data and statistics files.
- **Appendix D** (b) (4) **Human Factors Summative Study Report:** This file is too large to email. It will be included in the complete ecopy to be delivered to the DCC tomorrow.
- **References:** These will be included in the complete ecopy to be delivered to the DCC tomorrow.

Please confirm receipt. I am not sure if the attachment is too large. If so, I can break it into multiple emails.

Kind Regards,
Calley

Please note: I will be out of the office Aug 17 - 23
Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct

cherzog@biologicsconsulting.com
BiologicsConsulting.com

From: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Sent: Wednesday, August 8, 2018 7:51 AM
To: Calley Herzog <cherzog@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: RE: (b) (4) - de novo documents

Calley,

After a cursory review of the email contents you provided there seem to be some documents missing that we had expected to be in the submission. The missing documents are:

- Revised hazards analysis
- Software Testing (V&V)
- Traceability Analysis
- Unresolved Anomalies
- Revision level history
- OTS (Off the Shelf Software) documentation

I recognize that the email you provided may not necessarily be an exhaustive list of documents that are arriving in the official submission. However, we will need these documents for the substantive review of the (b) (4) app. Please let me know if you have any questions and when we can expect to have these documents for review.

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Calley Herzog [mailto:cherzog@biologicsconsulting.com]
Sent: Tuesday, August 7, 2018 3:41 PM
To: Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: (b) (4) - de novo documents

Erdit,

As promised, I am providing the following (b) (4) documents as attachments to this email:

- De novo main body
- Appendix I – SRS (both clean and redlined)
- Appendix J – SDS
- Appendix P – responses to FDA Questions

These documents, along with all remaining appendices except for the clinical study report will be delivered to FDA as a de novo submission on Thursday (8/9). The clinical study report will be provided by email on Friday (8/10), followed by an ecopy delivered to FDA on Monday (8/13) as a supplement to the de novo.

Please let us know if you have any questions or concerns about the timeline or submission process.

Kind Regards,
Calley

Calley Herzog
Senior Consultant, Assistant Team Leader - Medical Devices
Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(720) 883.3633 – Direct
cherzog@biologicsconsulting.com
BiologicsConsulting.com

Lewis, LaToye

From: Gremi, Erdit
Sent: Tuesday, August 21, 2018 6:30 PM
To: 'Donna-Bea Tillman'; 'Calley Herzog'
Cc: Paulsen, Jessica; Ricci, Linda J
Subject: RE: DEN180042 Software Concerns

Donna-Bea,

(b) (4)

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Gremi, Erdit
Sent: Tuesday, August 21, 2018 7:52 AM
To: 'Donna-Bea Tillman' <dtillman@biologicsconsulting.com>; 'Calley Herzog' <cherzog@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Subject: DEN180042 Software Concerns

Donna-Bea

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Thank you,

Erdit Gremi
Lead Reviewer
CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Gremi, Erdit

From: Gremi, Erdit
Sent: Tuesday, August 28, 2018 9:14 AM
To: 'Donna-Bea Tillman'; Ricci, Linda J; Paulsen, Jessica; Cruz, Marisa
Cc: Drummond, Arielle
Subject: RE: interactive review

Donna-Bea,

Can we get more information on (b) (6) ? The SAEs for this subject include:

(b) (6)
Chest pain
Could not breath
Unconscious
Unexplained death

Is there a reason why this patient did not appear to seek medical treatment despite having SAEs 3-4 days prior to the unexplained death while using the device? Did the watch provide any AF alert notifications during the time of the SAEs?

Eri Gremi

WO66 Room:1102
Tel: 240-402-3910

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Monday, August 27, 2018 8:27 PM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Attached please find the second item that was due today: Additional Information from the AHS study.

The final item for today will be sent directly to you by my client.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 6:17 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; 'Paulsen, Jessica' <Jessica.Paulsen@fda.hhs.gov>; 'Cruz, Marisa' <Marisa.Cruz@fda.hhs.gov>; 'Gremi, Erdit' <Erdit.Gremi@fda.hhs.gov>
Cc: 'Drummond, Arielle' <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA team:

Attached please find the first of the items due today: Additional information for (b) (4) Intended Use population (Aug. 23 email).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 1:18 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Here is the updated status on outstanding items:

Items to be provided by end of today (August 27)
- Responses to (b) (4) questions (Aug. 22 email)
- Additional information in (b) (4) Intended Use population (Aug. 23 email)
- Additional data from AHS study

Items to be provide by end of the day tomorrow (August 28)
- Responses to (b) Clinical/Performance questions (August 24 email)
- (b) Validation for the platform input to the app

In regards to (b) (4) Validation for the platform input to the app, we will let you know by the end of the day today when we expect to have that information.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Monday, August 27, 2018 11:55 AM
To: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: interactive review

Hello Donna-Bea,

We would like to see where we are with the requests for:

- Validation data for the input to each of the apps (b) (4)
- Timing for responses to outstanding issues
- Timing for AHS data request

Please either provide an update via email before 1 or we can discuss at 1. If you can provide by email, then we are comfortable cancelling the 1pm call.

Thanks!
--Linda

Linda Ricci
Associate Director ODE DH

Center for Devices and Radiologic Health
Office of Device Evaluation
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

Excellent customer service is important to us. Please take a moment to provide feedback regarding the customer service you have received: https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Monday, August 27, 2018 6:17 PM
To: Ricci, Linda J; Paulsen, Jessica; Cruz, Marisa; Gremi, Erdit
Cc: Drummond, Arielle
Subject: RE: interactive review
Attachments: (b) (4) Intended Use Population.pdf

FDA team:

Attached please find the first of the items due today: Additional information for (b) (4) Intended Use population (Aug. 23 email).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 1:18 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Here is the updated status on outstanding items:

Items to be provided by end of today (August 27)
- Responses to (b) (4) questions (Aug. 22 email)
- Additional information in (b) (4) Intended Use population (Aug. 23 email)
- Additional data from AHS study

Items to be provide by end of the day tomorrow (August 28)
- Responses to (b) Clinical/Performance questions (August 24 email)
- Spice: Validation for the platform input to the app

In regards to (b) (4) Validation for the platform input to the app, we will let you know by the end of the day today when we expect to have that information.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Monday, August 27, 2018 11:55 AM
To: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: interactive review

Hello Donna-Bea,

We would like to see where we are with the requests for:

- Validation data for the input to each of the apps (b) (4) [redacted]
- Timing for responses to outstanding issues
- Timing for AHS data request

Please either provide an update via email before 1 or we can discuss at 1. If you can provide by email, then we are comfortable cancelling the 1pm call.

Thanks!
--Linda

Linda Ricci
Associate Director ODE DH

Center for Devices and Radiologic Health
Office of Device Evaluation
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

Excellent customer service is important to us. Please take a moment to provide feedback regarding the customer service you have received: https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Gremi, Erdit

From: Gremi, Erdit
Sent: Tuesday, August 28, 2018 2:37 PM
To: 'Donna-Bea Tillman'; Ricci, Linda J; Paulsen, Jessica; Cruz, Marisa
Cc: Drummond, Arielle
Subject: RE: interactive review

Donna-Bea,

(b) (4)

[redacted]

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Monday, August 27, 2018 8:27 PM
To: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Attached please find the second item that was due today: Additional Information from the AHS study.

The final item for today will be sent directly to you by my client.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting

PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 6:17 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; 'Paulsen, Jessica' <Jessica.Paulsen@fda.hhs.gov>; 'Cruz, Marisa' <Marisa.Cruz@fda.hhs.gov>; 'Gremi, Erdit' <Erdit.Gremi@fda.hhs.gov>
Cc: 'Drummond, Arielle' <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA team:

Attached please find the first of the items due today: Additional information for (b) (4) Intended Use population (Aug. 23 email).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 1:18 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Here is the updated status on outstanding items:

Items to be provided by end of today (August 27)

- Responses to (b) (4) questions (Aug. 22 email)
- Additional information in (b) (4) Intended Use population (Aug. 23 email)
- Additional data from AHS study

Items to be provide by end of the day tomorrow (August 28)

- Responses to (b) Clinical/Performance questions (August 24 email)
- (b) Validation for the platform input to the app

In regards to (b) (4) Validation for the platform input to the app, we will let you know by the end of the day today when we expect to have that information.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Monday, August 27, 2018 11:55 AM
To: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: interactive review

Hello Donna-Bea,

We would like to see where we are with the requests for:

- Validation data for the input to each of the apps (b) (4)
- Timing for responses to outstanding issues
- Timing for AHS data request

Please either provide an update via email before 1 or we can discuss at 1. If you can provide by email, then we are comfortable cancelling the 1pm call.

Thanks!
--Linda

Linda Ricci
Associate Director ODE DH

Center for Devices and Radiologic Health
Office of Device Evaluation
U.S. Food and Drug Administration

Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

Excellent customer service is important to us. Please take a moment to provide feedback regarding the customer service you have received: https://www.research.net/s/cdrhcustomerservice?O=400&D=440&B=442&E=&S=E

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Monday, August 27, 2018 8:27 PM
To: Ricci, Linda J; Paulsen, Jessica; Cruz, Marisa; Gremi, Erdit
Cc: Drummond, Arielle
Subject: RE: interactive review
Attachments: AHS Data Response.pdf

FDA Team:

Attached please find the second item that was due today: Additional Information from the AHS study.

The final item for today will be sent directly to you by my client.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 6:17 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; 'Paulsen, Jessica' <Jessica.Paulsen@fda.hhs.gov>; 'Cruz, Marisa' <Marisa.Cruz@fda.hhs.gov>; 'Gremi, Erdit' <Erdit.Gremi@fda.hhs.gov>
Cc: 'Drummond, Arielle' <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA team:

Attached please find the first of the items due today: Additional information for (b) (4) Intended Use population (Aug. 23 email).

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com

From: Donna-Bea Tillman
Sent: Monday, August 27, 2018 1:18 PM
To: 'Ricci, Linda J' <Linda.Ricci@fda.hhs.gov>; Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: RE: interactive review

FDA Team:

Here is the updated status on outstanding items:

Items to be provided by end of today (August 27)

- Responses to (b) (4) questions (Aug. 22 email)
- Additional information in (b) (4) Intended Use population (Aug. 23 email)
- Additional data from AHS study

Items to be provide by end of the day tomorrow (August 28)

- Responses to (b) Clinical/Performance questions (August 24 email)
- (b) Validation for the platform input to the app

In regards to (b) (4) Validation for the platform input to the app, we will let you know by the end of the day today when we expect to have that information.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Monday, August 27, 2018 11:55 AM
To: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Donna-Bea Tillman <dtillman@biologicsconsulting.com>; Cruz, Marisa <Marisa.Cruz@fda.hhs.gov>
Cc: Drummond, Arielle <Arielle.Drummond@fda.hhs.gov>
Subject: interactive review

External (linda.ricci@fda.hhs.gov)

Hello Donna-Bea,

We would like to see where we are with the requests for:

- Validation data for the input to each of the apps (b) (4) [redacted]
- Timing for responses to outstanding issues
- Timing for AHS data request

Please either provide an update via email before 1 or we can discuss at 1. If you can provide by email, then we are comfortable cancelling the 1pm call.

Thanks!
--Linda

Linda Ricci
Associate Director ODE DH

Center for Devices and Radiologic Health
Office of Device Evaluation
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Friday, August 31, 2018 9:07 AM
To: Ricci, Linda J
Cc: Paulsen, Jessica; Gremi, Erdit; Ralston, Luke
Subject: RE: meeting today

Thanks for the heads up. We will make sure to have the right people on the call.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

From: Ricci, Linda J <Linda.Ricci@fda.hhs.gov>
Sent: Friday, August 31, 2018 9:04 AM
To: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Cc: Paulsen, Jessica <Jessica.Paulsen@fda.hhs.gov>; Gremi, Erdit <Erdit.Gremi@fda.hhs.gov>; Ralston, Luke <Luke.Ralston@fda.hhs.gov>
Subject: meeting today

Hi Donna-Bea,

We would like to discuss the following at the meeting today at 1:

1. Statistical results of the (b) study – we are trying to understand the scatter plots. Would be great to have someone on the call that can help us interpret these.
2. Remaining (b) software deficiencies
3. (b) IFU

Linda Ricci
Associate Director ODE DH

Office of Device Evaluation
Center for Devices and Radiologic Health
U.S. Food and Drug Administration
Tel: 301-796-6325
Linda.Ricci@fda.hhs.gov

(OPEQ Pilot: Immediate Office/Regulations, Policy, and Guidance Staff)
Excellent customer service is important to us. Please take a moment to provide feedback regarding the customer service you have received**:** https://www.research.net/s/cdrhcustomerservice?ID=1040&S=E

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

Gremi, Erdit

From: Gremi, Erdit
Sent: Friday, August 17, 2018 8:58 PM
To: 'Donna-Bea Tillman'; 'Calley Herzog'
Cc: Ricci, Linda J; Paulsen, Jessica
Subject: Statistical and Algorithm design concerns

Donna Bea,

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

(b)(4) Specifications

[redacted]

Thank you,

Erdit Gremi
Lead Reviewer

CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices Branch
U.S. Food and Drug Administration
OPEQ Pilot: **Office of Health Technology 2 | Division of Health Technology 2A | External Heart Rhythm and Rate Devices Team**

WO66 Room:1102
Tel: 240-402-3910
Erdit.Gremi@fda.hhs.gov

Lewis, LaToye

From: Donna-Bea Tillman <dtillman@biologicsconsulting.com>
Sent: Wednesday, August 29, 2018 10:11 PM
To: Ricci, Linda J; Paulsen, Jessica; Drummond, Arielle; Gremi, Erdit
Subject: Updated QA Test Report for (b) (4) AF Gate
Attachments: (b) (4) _1.0.2_-results.pdf

FDA Team:

Attached find the test report which verifies version 1.0.2 of (b) (4) which includes the AF gate functionality. Please recall that we sent the updated SRS, Device Hazard Analysis, and Traceability Matrix which included this change to you on August 24.

Donna-Bea

Donna-Bea Tillman, Ph.D, FRAPS
Team Leader and Senior Consultant, Medical Devices

Biologics Consulting
PHARMACEUTICALS DEVICES BIOLOGICS
(410) 531-6542 - Direct
(703) 739.5695 – Main Office
dtillman@biologicsconsulting.com
BiologicsConsulting.com

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

Irregular Rhythm Notification Feature

Instructions for Use

Apple Inc.
One Apple Park Way
Cupertino, CA 95014
www.apple.com

Revision [X]

[REVISION DATE]

INDICATIONS FOR USE

The Irregular Rhythm Notification Feature is a software-only mobile medical application that is intended to be used with the Apple Watch. The feature analyzes pulse rate data to identify episodes of irregular heart rhythms suggestive of atrial fibrillation (AFib) and provides a notification to the user. The feature is intended for over-the-counter (OTC) use. It is not intended to provide a notification on every episode of irregular rhythm suggestive of AFib and the absence of a notification is not intended to indicate no disease process is present; rather the feature is intended to opportunistically surface a notification of possible AFib when sufficient data are available for analysis. These data are only captured when the user is still. Along with the user's risk factors, the feature can be used to supplement the decision for AFib screening. The feature is not intended to replace traditional methods of diagnosis or treatment.

The feature has not been tested for and is not intended for use in people under 22 years of age. It is also not intended for use in individuals previously diagnosed with AFib.

USING THE IRREGULAR RHYTHM NOTIFICATION FEATURE

Set-Up/On-boarding

- The Irregular Rhythm Notification Feature is available on Apple Watch Series 1-4 with watchOS 5.1 or later, paired with iPhone 5s or later with iOS 12.1 or later.
- Open the Health app on your iPhone.
- In the Health Data tab, tap Heart, then select "Irregular Rhythm Notifications."

- Follow the onscreen instructions.
- You may exit on-boarding at any time by pressing “Cancel.”

Receiving a Notification

- Once the feature is turned on, you will receive a notification if the feature identified a heart rhythm suggestive of AFib and confirmed it on multiple readings.
- If you have not been diagnosed with AFib by a physician, you should discuss the notification with your doctor.

All data collected and analyzed by the Irregular Rhythm Notification Feature is saved to the Health app on your iPhone. If you choose to, you can share that information by exporting your health data in the Health app.

New data cannot be collected once your Apple Watch’s storage is full. You should free up space by deleting unwanted apps, music or podcasts. You can check your storage usage by navigating to the Apple Watch app on your iPhone, clicking “My Watch”, clicking “General”, and then clicking “Usage”.

SAFETY AND PERFORMANCE

In a study of 226 participants aged 22 years or older who had received an AFib notification while wearing Apple Watch and subsequently wore an electrocardiogram (ECG) patch for approximately 1 week, 41.6% (94/226) had AFib detected by ECG patch. During concurrent wear of Apple Watch and an ECG patch, 57/226 participants received an AFib notification. Of those, 78.9% (45/57) showed concordant AFib on the ECG patch and 98.2 % (56/57) showed AFib and other clinically relevant arrhythmias. These results demonstrate that, while in the majority of cases the notification will accurately represent the presence of AFib, in some instances, a notification may indicate the presence of an arrhythmia other than AFib. No serious device adverse effects were observed.

CAUTIONS

The Irregular Rhythm Notification Feature cannot detect heart attacks. If you ever experience chest pain, pressure, tightness, or what you think is a heart attack, call emergency services.

The Irregular Rhythm Notification Feature is not constantly looking for AFib and should not be relied on as a continuous monitor. This means the feature cannot detect all instances of AFib, and people with AFib may not get a notification.

Apple Watch may be unable to collect data when Apple Watch is in close vicinity to strong electromagnetic fields (e.g. electromagnetic anti-theft systems, metal detectors).

A number of factors can impact the ability of the feature to measure your pulse and detect an irregular rhythm suggestive of AFib. These include factors like motion, hand and finger movements, dark tattoos on the wrist, and the amount of blood flow to your skin (which can be reduced by cold temperatures).

DO NOT wear your Apple Watch during a medical procedure (e.g., magnetic resonance imaging, diathermy, lithotripsy, cautery and external defibrillation procedures).

DO NOT change your medication without talking to your doctor.

Not intended for use by individuals under age 22.

Not intended for use by individuals previously diagnosed with AFib.

Notifications made by this feature are potential findings, not a complete diagnosis of cardiac conditions. All notifications should be reviewed by a medical professional for clinical decision-making.

Apple does not guarantee that you are not experiencing an arrhythmia or other health conditions even in the absence of an irregular rhythm notification. You should notify your physician if you experience any changes to your health.

For best results, make sure your Apple Watch fits snugly on top of your wrist.
The heart rate sensor should stay close to your skin.

SECURITY: Apple recommends that you add a passcode (personal identification number [PIN]), Face ID or Touch ID (fingerprint) to your iPhone and a passcode (personal identification number [PIN]) to your Apple Watch to add a layer of security. It is important to secure the iPhone since you will be storing personal health information.

EQUIPMENT SYMBOLS

Manufacturer

Read instructions before use

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

Benefit-Risk Assessment: Decision Support Tool

Form
Applies To: CDRH
Date Effective: 06/20/2018

Use FEEDBACK✓CDRH to provide comments on this document (include Doc#01125)

	A. Proposed Indications for Use	B. Potential Modified Indications for Use and/or Population[1]
Level of Evidence Questions Based on the totality of the data Device Name: (b) (4) App PMA/De Novo Number: DEN180042 ☒ Interim ☐ Final	Proposed Indication for Use (IFU) – Column A: (b)(4) Draft	Click here to insert modified Indications for Use.
Assessment of Benefit	Considering benefit in terms of • Magnitude • Duration • Probability • Patient perspective	Considering benefit in terms of • Magnitude • Duration • Probability • Patient perspective
1. Is there any evidence of clinical benefit?	☒ YES → Q2 ☐ NO → move to column B	☐ YES → Q2 ☐ NO → Do not approve/grant
2. What is the degree of uncertainty for the benefits?	☐ High ☐ Med ☒ Low Continue to Q3	☐ High ☐ Med ☐ Low Continue to Q3
Assessment of Risk	Considering risk in terms of • Severity • Duration • Probability • Patient perspective	Considering risk in terms of • Severity • Duration • Probability • Patient perspective

[1] Instructions: Consider the benefits and risks for a modified Population for the proposed use, modified Indications for Use for the proposed population, or both modified Indications for Use and modified Population

3. Are known/probable risks more than minimal?	☐ YES → Q4 ☒ NO → Q4	☐ YES → Q4 ☐ NO → Q4
4. What is the degree of uncertainty for the Risks?	☐ High ☒ Med ☐ Low Continue to Q5	☐ High ☐ Med ☐ Low Continue to Q5
Assessment of Benefit-Risk		
5. Do the Benefits outweigh the Risks?	☒ YES → Approve/grant ☐ Undetermined → Q6	☐ YES → Approve/grant ☐ Undetermined → Q6
6. Do the Benefits outweigh the Risks, considering additional factors?	☐ YES → Approve/grant ☐ Undetermined → Q7	☐ YES → Approve/grant ☐ Undetermined → Q7
7. Can the risks be mitigated, so that Benefits outweigh the Risks?	☐ YES → Approve/grant ☐ Undetermined → Q8	☐ YES → Approve/grant ☐ Undetermined → Q8
8. Do the Benefits outweigh the Risks considering the use of postmarket actions?	☐ YES → Approve/grant ☐ NO → move to B	☐ YES → Approve/grant ☐ NO → Do not approve/grant

Level of Evidence Questions for Benefit-Risk Assessment

Form

Applies To: ODE and OIR

Date Effective: 06/20/2018

Use FEEDBACK✓CDRH to provide comments on this document (include Doc # 01126)

Purpose: This form is intended to serve as a complementary form to the Benefit-Risk Decision Support Tool to guide review staff regarding critical elements that should be considered as part of the thought-process associated with benefit-risk assessments. This form is intended for inclusion as part of the administrative record and also intended to facilitate management's review during the oversight process in order to ascertain which elements were considered by review staff.

Instructions: Consider questions 1-8 for Column A (the proposed Indication for Use), until you reach a recommendation to either approve/grant or move to Column B. When considering an acceptable, modified Indications for Use, interact with the sponsor to reach agreement on a modified Indication for Use.

Beta Testing Instructions: Send feedback concerning any issue identified as a result of using the revised B-R tools to Benefit-RiskTools@fda.hhs.gov. Upon completion of this form and the Decision Support Tool (when the documents are used as part of a management interim meeting or for supporting a final decision), email the completed documents to Benefit-RiskTools@fda.hhs.gov. Please note that Benefit-RiskTools@fda.hhs.gov is an internal email address for the purpose of the beta testing. Do not disseminate outside of CDRH.

Premarket Submission Type	☐ PMA ☒ De Novo
PMA/De Novo Number:	DEN180042
Device Name:	(b) (4) App
Applicant:	(b) (4)
Medical Officer:	Kan Fang, MD
Scientific Reviewer:	Erdit Gremi, MSE
Worksheet Completion Date:	8/28/2018
Review Stage:	☐ Interim (Complete Q1-4, select considerations, and explain in text boxes. There is no need to answer Yes/No for Q5-8.) ☒ Final (Complete Q1-5 and Q6-8, as needed.)
Device Description: The (b) (4) App comprises a pair of mobile medical apps, one on Apple Watch and the other on the iPhone.	

- The (b) (4) Watch App analyzes pulse rate data collected by the Apple Watch PPG sensor to identify episodes of irregular heart rhythms consistent with AF and provides a notification to the user. It is a background screening tool.
- The (b) (4) iPhone App is part of the Health App, which allows users to store, manage, and share health and fitness data, and comes pre-installed on every iPhone. It receives AF notifications from the (b) (4) Watch and displays a history of AF notifications. The App also provides access to educational information.

Proposed Indication for Use (IFU) – Column A:

(b)(4) Draft

[redacted]

Modified Indication for Use (if different than proposed) – Column B:
N/A

Assessment of Benefit

1. **Is there any evidence of clinical benefit?**

   Is a clinical benefit demonstrated for the device for this indication (e.g., from any one or more of the primary and/or secondary datasets or from associated real-world evidence)? Benefit may be considered in terms of how a patient feels, functions, survives, or an acceptable surrogate outcome. Benefit may also be considered in terms of convenience in managing or diagnosing a disease or condition. Benefit should be considered based on the clinical assessment of the data, whether or not the results are statistically significant. *Select any of the following that demonstrate benefit.*

A	B	A favorable change in at least 1 clinical assessment that:
☐	☐	Is equal to or greater than seen in the control group
☐	☐	Meets a predetermined performance goal
☐	☐	Meets or surpasses a minimally important clinical difference
☒	☐	Is equal to or greater than seen with other available modalities for the condition
☐	☐	Would be meaningful to patients considering the severity, chronicity, etc., of the condition, taking into consideration patient-reported outcomes and health-related quality of life

☐ ☐ A favorable change in non-clinical data or modeling that is deemed to be predictive of clinical outcomes
☒ ☐ A favorable clinical performance characteristic (e.g., sensitivity/PPA,[1] specificity/NPA[2], etc.) for the screening, diagnosis, prognosis, monitoring or treatment selection
☐ ☐ Acceptable performance characteristics for analytical validation of the device
☐ ☐ Other(s) Click here to list other(s)
☐ ☐ None

Q1: Is there any evidence of clinical benefit?

A B
☒ ☐ YES → Continue to Question 2
☐ ☐ NO → Move one column to the right (or, if final column has been reached and you have determined there is no evidence of clinical benefit, do not approve the application/request)

[1] PPA: Positive Percent Agreement
[2] NPA: Negative Percent Agreement

2. What is the degree of uncertainty for the benefits?

Recognizing that some degree of uncertainty always exists, select the sources of uncertainty, if applicable, in the data that affect your assessment of the clinical benefit. Consider sensitivity, specificity, accuracy, precision, reproducibility, etc. (analytical and/or clinical validation, as applicable).

A	B	
☐	☐	Inconsistent or conflicting results between studies
☐	☐	Wide confidence intervals surrounding the point estimate(s) and/or odds ratio(s))
☐	☐	A significantly underpowered study with statistical insignificance in outcome measure(s)
☐	☐	High subject or specimen loss-to-follow-up at critical assessment point(s)
☐	☐	Large amount of missing data at critical assessment time(s) +/- imputation
☐	☐	Significant number of major protocol deviations
☐	☐	Impact of confounding interventions or physiological factors
☐	☐	Inconsistent user experience or user experience not representative of likely real world user
☐	☐	Unclear correlation between non-clinical data, pre-selected enriched data, or computer modeling and clinical performance
☐	☐	Surrogate endpoint has not yet been demonstrated to correlate with a clinical outcome
☐	☐	Real World Evidence (RWE) is not relevant or reliable for the purposes of the proposed analysis
☐	☐	Inspectional findings
☒	☐	Study design or results lead to lack of generalizability for the intended use population or specific clinical subpopulations.
☐	☐	Physiological or clinically meaningful range of the diagnostic output is unknown or generalizability of proposed clinical cut-off is unknown
☐	☐	Imperfect comparator method used to calculate performance characteristics
☐	☐	Other(s) Click here to list other(s)
☐	☐	None

Q2: What is the degree of uncertainty for the benefits?

A	B	
☒	☐	Low → Continue to Question 3
☐	☐	Med → Continue to Question 3
☐	☐	High → Continue to Question 3

Summary of the Assessment of Benefit

For the Proposed Indications for Use (Column A):

(b)(5) FDA Draft

[redacted]

(b)(5) FDA Draft

For a modified Indications for Use (modified indication and/or population) (Column B):

N/A

3. Are known/probable risks more than minimal?

Select the elements that apply for known/probable risks that are more than minimal.

A B

☐ ☐ Adverse events (AEs) or outcomes related to the device itself

☐ ☐ AEs or outcomes related to the use of the device or procedure to use the device

☐ ☐ AEs or outcomes related to anesthesia or sedation to use the device

☐ ☐ AEs or outcomes due to subsequent tests/treatments needed (e.g., radiation from CT scans)

☐ ☐ AEs or outcomes, not seen in the study/data, but probable based on "class effect" or events known to occur with similar technologies

☒ ☐ False positive/false negative/failed to provide a result for diagnostics

☐ ☐ Treatment or diagnostic intended to be used as a standalone rather than an adjunctive use

☒ ☐ Other(s): Human use errors (misinterpreting the function of the device), may include

- Symptomatic users falsely reassured and delay seeking evaluation
- Self-medicating or changing disease management based on the device output.

☐ ☐ None

Q3: Are known/probable risks more than minimal?

A B

☐ ☐ YES → Continue to Question 4

☒ ☐ NO → Continue to Question 4

4. What is the degree of uncertainty for the risks?

Recognizing that some degree of uncertainty always exists, select the sources uncertainty, if applicable, in the data regarding the adverse events/outcomes or risks.

A	B	
☐	☐	Insufficient patient numbers to detect serious events or false positives/false negatives
☐	☐	Insufficient duration of follow-up to detect delayed/late events
☐	☐	Lack of data on repeated exposure to the device/use
☐	☐	Inconsistent or conflicting results between studies
☒	☐	Proper evaluations not performed as part of the study protocol to adequately detect certain AEs
☐	☐	Poor or inconsistent adverse event definitions and documentation
☐	☐	Events likely confounded by, and attributed to, other comorbidities or treatment modalities
☐	☐	High subject loss-to-follow-up at critical assessment point(s)
☐	☐	Large amount of missing data at critical assessment time(s) +/- imputation
☐	☐	Significant number of major protocol deviations
☐	☐	Inconsistent user experience or user experience not representative of likely real world user
☐	☐	Concerns related to performance characteristics (e.g., sensitivity/PPA, specificity/NPA)
☐	☐	Imperfect comparator method used to calculate performance characteristics
☐	☐	Other(s) Click here to list other(s)
☐	☐	None

Q4: What is the degree of uncertainty for the risks?

A	B	
☐	☐	Low → Continue to Question 5
☒	☐	Med → Continue to Question 5
☐	☐	High → Continue to Question 5

Summary of the Assessment of Risk

For the Proposed Indications for Use (Column A):

(b)(5) FDA Draft

[redacted]

(b)(5) FDA Draft

[redacted]

For a modified Indications for Use (modified indication and/or population) (Column B):

N/A

Assessment of Benefit-Risk

At interim stage, it is not necessary to select "yes" or "no" for questions 5-8. Select the relevant considerations and explain in text boxes.

To approve a PMA application or grant a De Novo Request, FDA must find, among other things, that the device is reasonably safe and effective. FDA determines whether there is a reasonable assurance of safety and effectiveness by weighing any probable benefit to health from the use of the device against any probable risk of injury or illness for such use, among other relevant factors.

5. **Do the Benefits outweigh the Risks, considering the assessment of Benefit and Risk and the degrees of uncertainty identified above?**

A B

☒ ☐ Yes – the benefits outweigh the risks such that, for this device, additional consideration of relevant factors would not change that determination – approve/grant

☐ ☐ Undetermined – the benefits may not outweigh the risks, and further discussion and consideration of relevant factors is appropriate – Move to Q6

Summary of the Assessment of Benefit-Risk

For the Proposed Indications for Use (Column A):

(b)(5) FDA Draft

[redacted]

For a modified Indications for Use (modified indication and/or population) (Column B):

Click here to summarize the clinical benefit(s) that have been demonstrated for a modified Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how uncertainty regarding Benefit(s) and Risks affects your assessment.

6. **Do the Benefits outweigh the Risks, when considering the following additional factors?** *Select relevant considerations.*

A	B	
☐	☐	Understanding of patient willingness to accept a large degree of uncertainty of the benefits or risks
☐	☐	Available patient preference information (PPI) showing patient willingness or unwillingness to accept the probable risks in exchange for the probable benefits
☐	☐	Available qualitative or quantitative PPI on the relative desirability or acceptability to patients of outcomes or other attributes that differ among alternative health interventions
☐	☐	Understanding that the device represents novel technology for which the current device technology is different

A	B	
☐	☐	Ability to manage or diagnose the condition and consideration of natural history of disease progression in the absence of the intervention or diagnostic information with the device under review
☐	☐	No legally marketed alternative medical product or medical intervention exists or the device offers advantages over existing alternatives
☐	☐	The device fills an unmet medical need or niche for more effective treatment or diagnosis of life-threatening or irreversibly debilitating human disease/conditions
☐	☐	The adverse events associated with use of the device are reversible
☐	☐	Type of intervention required to address the harmful event (e.g., medication, surgery)
☐	☐	The study is a first of a kind (robustness of the analysis)
☐	☐	Tipping point and/or worst-case sensitivity analysis continuing to show clinical benefit
☐	☐	Understanding of mechanistic plausibility and/or "class effect" (e.g., familiarity with similar technology)
☐	☐	Other(s) Click here to list other(s)
☐	☐	None

Q6: Do the Benefits outweigh the Risks, when considering the additional factors?

A	B	
☐	☐	Yes – the benefits outweigh the risks such that, for this device, additional consideration of relevant factors would not change that determination – approve/grant
☐	☐	Undetermined – the benefits may not outweigh the risks, and further discussion and consideration of risk mitigation measures is appropriate – Move to Q7

Summary of the Assessment of Benefit-Risk, taking into account additional relevant considerations

For the Proposed Indications for Use (Column A):

Click here to summarize the clinical benefit(s) that have been demonstrated for the proposed Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their probable benefits and risks, affect your assessment.

Include a description of how uncertainty regarding Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

For a modified Indications for Use (modified indication and/or population) (Column B):
Click here to summarize the clinical benefit(s) that have been demonstrated for a modified Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their probable benefits and risks, affect your assessment. Include a description of how uncertainty regarding Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

7. **Can the risks be mitigated, so that Benefits outweigh the Risks? Consider if the Benefits outweigh the Risks if risk mitigation strategies are incorporated to lower the probability of a harmful event occurring and improve the benefit-risk profile of the device.** *Select relevant considerations.*

A B
☐ ☐ Additional description of known and probable benefits and risks in physician and patient labeling including adequate Contraindications, Warnings, and Precautions and description of the clinical events
☐ ☐ Additional warnings noting limitations of safety information (e.g., "The safety of the use of this device in [situation] has not been evaluated.")
☐ ☐ Labeling the device "Prescription Only"
Training:
☐ ☐ Limitation to caregivers with certain qualifications or clinical training
☐ ☐ Limit to users with a minimum set of qualifications and/or training
☐ ☐ Physician/user training program
Other:
☐ ☐ Device tracking
☐ ☐ Other(s) Click here to list other(s)
☐ ☐ None

Q7: Can the risks be mitigated, so that Benefits outweigh the Risks?

A B
☐ ☐ Yes – the benefits outweigh the risks such that, for this device, additional consideration of relevant factors would not change that determination – approve/grant
☐ ☐ Undetermined – the benefits may not outweigh the risks, and further discussion and consideration of postmarket actions is appropriate – Move to Q8

Summary of the Assessment of Benefit-Risk, considering risk mitigation strategies

For the Proposed Indications for Use (Column A):
Click here to summarize the clinical benefit(s) that have been demonstrated for the proposed Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their benefits and risks, affect your assessment. Include

a description of how uncertainty regarding Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

For a modified Indications for Use (modified indication and/or population) (Column B):
Click here to summarize the clinical benefit(s) that have been demonstrated for a modified Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their benefits and risks, affect your assessment. Include a description of how uncertainty regarding Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

8. **Do the Benefits outweigh the Risks considering the use of postmarket actions?** *Select appropriate postmarket action(s).*

A	B	
☐	☐	Collection of additional and/or confirmatory non-clinical performance data in the postmarket space
☐	☐	Collection of additional and/or confirmatory clinical data in the postmarket space
☐	☐	Actions taken in response to inspectional findings (waiver/variance)
☐	☐	Other(s) Click here to list other(s)
☐	☐	None

Q8: Do the Benefits outweigh the Risks considering the use of postmarket actions?

A	B	
☐	☐	Yes – Approve/grant
☐	☐	No – If the benefits do not outweigh the risks, move to the right column in the matrix to assess the benefits and risks for modified indications (or if the final column has been reached, do not approve/grant).

Summary of the Assessment of Benefit-Risk, considering postmarket actions

For the Proposed Indications for Use (Column A):
Click here to summarize the benefit(s) that have been demonstrated for the proposed Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their probable benefits and risks, affect your assessment. Include a description of how uncertainty regarding Probable Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

For a modified Indications for Use (modified indication and/or population) (Column B):
Click here to summarize the benefit(s) that have been demonstrated for a modified Indications for Use and your assessment of how Benefit(s) compare to Risks. Include a description of how available alternative modalities, including their probable benefits and risks, affect your assessment. Include a description of how uncertainty regarding Probable Benefit(s) and Risks affects your assessment. Include a description of how patient perspectives affected your assessment.

[END OF FORM or TEMPLATE – REMOVE CONTENT FROM THIS LINE TO END OF DOCUMENT PRIOR TO PUBLISHING]

Change Control, Change History

Change Control Table

Version	Document Author, Title	Document Approver, Title, Office	Date Approved
2.00	Jonette Foy, PhD, Associate Director for Policy	Jeff Shuren, MD, JD, Center Director	06/14/2018
1.00	Jonette Foy, PhD, Associate Director for Policy (Acting)	Jeff Shuren, MD, JD, Center Director	09/07/2017

Complete Change Control Table (all versions) retained in SWIFT Docs.

Change History

Version	Description of Changes	Form ID	Date Effective
2.00	Collapsed columns B-D into one column B; streamlined questions to align with broader device portfolio (no separate questions for non-therapeutic/non-invasive diagnostics); added instructions for this document at the interim stage and other clarifying text	01103.02.01	06/20/2018
1.00	Initial Controlled Version.	01103.01.01	10/01/2017

Change History (all versions) retained in SWIFT Docs.

DEN180042 – (b) (4) – (b) (4) [PPG based AF detection]

Date: Wednesday, September 05, 2018

Consultant: Loriano Galeotti, PhD
(FDA / CDRH / Office of Device Evaluation / Division of Cardiovascular Devices / Cardiac Diagnostic Devices)

Lead reviewer: Erdit Gremi.

Loriano Galeotti
Digitally signed by Loriano Galeotti -S
Date: 2018.09.05 18:11:33 -04'00'

Instructions/comments from Lead Reviewer: TBD.

Scope: This memo covers engineering aspects of the device related to the detection of Atrial Fibrillation. Other aspects are not reviewed unless otherwise noted.

Note: this memo and deficiencies are intended for internal discussion only, and should not be communicated to the sponsor unless otherwise indicated. Minor edits can be made to the deficiencies, in case of doubt or major edits, please contact the consultant.
Color coding (unless otherwise specified): plain font my comment; *italics* quotes from the sponsor; highlight: red = inadequate, green = adequate, yellow=comment to the lead reviewer;

Unless otherwise noted, references that do not specify a source document or indicating "denovo", "de-novo" "main" or similar are intended to the document "002_(b) (4) App - De Novo" dated Aug 7 2018 in DEN180042\ORIGINAL\VOL_001_COVER LETTER AND MAIN BODY. Unless otherwise specified, to "appendix" or "App" are to the corresponding appendices in DEN180042\ORIGINAL\VOL_002_APPENDICES unless otherwise noted; references to literature (e.g., ref_xx or ref xx) is to DEN180042\ORIGINAL\VOL_003_REFERENCES.

When referencing "this" submission, I'm meaning the current submission under review as indicated in the header of the present document, unless otherwise specified.

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

Deficiencies

Deficiencies in this section can be communicated to the sponsor.

Please review any deficiency for language, contents, and consistency with other deficiencies.)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

(b)(5) FDA Internal Deliberations

FOOD AND DRUG ADMINISTRATION
CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

OFFICE OF DEVICE EVALUATION
De Novo CLINICAL REVIEW

Date:	August 30, 2018	**Branch:**	CDDB
To:	Erdit Gremit, MSE Lead reviewer	**Division:**	DCD
From:	Kan Fang, MD. CDRH/ODE/DCD/CEDB		
cc:	Jessica Paulsen, Branch chief, IEDB		
	Mark Fellman, Branch chief, CEDB		
File:	DEN180042		
Purpose:	Clinical Review Memo		
Applicant:	(b) (4)		
Device/Study:	(b) (4) App		

Recommendation: Approval

(b)(5) FDA Internal Deliberations

[redacted]

(b)(4) Draft

[redacted]

(b)(4) Draft

Review Summary and Conclusion

The (b) (4) app is a medical software app that analyzes pulse rate data intermittently collected by the Apple Watch PPG sensor alerts the user when episodes of irregular heart rhythms suggestive of atrial fibrillation have been identified. It is an over-the-counter device intended for opportunistic AF screening. Apple has provided the following Indications for Use statement:

(b)(4) Draft

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

[redacted]

Human Factors (HF) Consult Memo

Consult Number:	CON1819669
Document Number:	DEN180042
Applicant:	(b) (4)
Trade Name:	(b) (4) App
Consult Type:	Human Factors
Requestor:	Erdit Gremi [ERDIT.GREMI] erdit.gremi@fda.hhs.gov ; 240-402-5880
Requestor Home:	CDRH\ OHT2\ DHT2A\ THT2A3
Requested Consultant:	
Gatekeeper / Consultant:	Kimberly Kontson [KIMBERLY.KONTSON] kimberly.kontson@fda.hhs.gov ; 301-796-4990
Consultant Home:	CDRH\ OSEL\ DBP
Date Requested:	August 13, 2018
Due Date:	August 17, 2018
Instructions:	HF/U review of the (b) (4) de novo application.

Indications for use:

(b)(4) Draft

[redacted]

Key considerations for conducting a HF review: Is the supporting documentation adequate to demonstrate that the subject device UI supports safe & effective use?

Date consult sent: August 17, 2018; Updated consult on 8/28/18 with sponsor responses and HF feedback from interactive review

(b)(4) Test Data

[redacted]

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

(b)(4) Test Data

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

MEMORANDUM

DATE: September 8, 2018
FROM: Linda Ricci
Associate Dir Digital Health, ODE

TO: DEN180042
Irregular Rhythm Notification Feature ([b) (4)

Linda J. Ricci -S
2018.09.08 12:17:26 -04'00'
Linda Ricci

I. INTRODUCTION

The indications for use are:

> The Irregular Rhythm Notification Feature is a software-only mobile medical application that is intended to be used with the Apple Watch. The feature analyzes pulse rate data to identify episodes of irregular heart rhythms suggestive of atrial fibrillation (AFib) and provides a notification to the user. The feature is intended for over-the-counter (OTC) use. It is not intended to provide a notification on every episode of irregular rhythm suggestive of AFib and the absence of a notification is not intended to indicate no disease process is present; rather the feature is intended to opportunistically surface a notification of possible AFib when sufficient data are available for analysis. These data are only captured when the user is still. Along with the user's risk factors, the feature can be used to supplement the decision for Afib screening. The feature is not intended to replace traditional methods of diagnosis or treatment.
>
> The feature has not been tested for and is not intended for use in people under 22 years of age. It is also not intended for use in individuals previously diagnosed with AFib.

Details of the software review are well documented in Nathalie Yarkony's memo. Dr. Yarkony provided a very thorough and scientifically based assessment of the submission.

The purpose of this memo is to document and assess the interactive review elements related to software, address the remaining software deficiencies identified by Dr. Yarkony and provide a final software assessment.

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

[redacted]

III. Conclusion

As documented above, I believe that the sponsor has addressed all of the remaining software deficiencies and from a software perspective, the file can be granted.

MEMO OF

SOFTWARE REVIEW

of a Moderate Level of Concern device

(b) (4)

De-Novo : DEN180042

Date : August 25, 2018

To : Erdit Gremi (CDRH/ODE/DCD/CDDB)

From : Nathalie Yarkony (CDRH/ODE/DCD/CDDB)

Sponsor (b) (4)

Device Name : (b) (4)

Review Summary

(b) (4)

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

(b)(4) Software Specifications

Date: September 4, 2018

From: Xuan Ye, Ph.D., Mathematical Statistician
Arkendra De, Ph.D., Mathematical Statistician
Division of Biostatistics, OSB/CDRH

Xuan Ye -S
Digitally signed by Xuan Ye -S
Date: 2018.09.04 12:07:55 -04'00'

Arkendra K. De -S
Digitally signed by Arkendra K. De -S
DN: c=US, o=U.S. Government, ou=HHS, ou=FDA, ou=People, cn=Arkendra K. De -S, 0.9.2342.19200300.100.1.1=1300405232
Date: 2018.09.04 11:45:49 -04'00'

Subject: Final Statistical Review of DEN180042, (b) (4) App, by (b) (4)

To: Erdit Gremi, Lead Reviewer
OHT2\DHT2A\THT2A3

CC: DBS Reviews

1. Background

On August 17, 2018, an initial statistical review memo for this submission was sent to the lead reviewer. Subsequently, there have been multiple interactions with the sponsor via interactive review. Interactive review responses related to the statistical concerns raised in the initial review have been provided to the lead reviewer. Please see the e-mails for this submission dated August 20, 2018; August 22, 2018; August 23, 2018; August 29, 2018 for the complete details of the responses to the statistical concerns. The aim of this review is to summarize the concerns provided in these e-mails as well as to describe any other remaining statistical concerns for this submission.

(b) (4)

(b) (4)

(b) (4)

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

MEMORANDUM

DATE: September 11, 2018

FROM: Bram D. Zuckerman, MD
Director, Division of Cardiovascular Devices

TO: DEN180042 – Irregular Rhythm Notification Feature (b) (4)

RECOMMENDATION: GRANTED (GRNT)

Bram D. Zuckerman -S
2018.09.11 13:49:54 -04'00'
Bram D. Zuckerman, MD

I. INTRODUCTION

The Irregular Rhythm Notification Feature (previously referred to as (b) (4) analyzes pulse rate data collected by the Apple Watch PPG sensor to identify episodes of irregular heart rhythms suggestive of AF and provides a notification to the user. (b) (4)

The regulatory history and review are well documented in the administrative file and summarized in Erdit Gremi's Lead Review Memo, dated September 6, 2018. The reviewer has recommended a Decline (DEND) decision on the file.

On September 7, 2018, the sponsor amended the file to update the official sponsor from (b) (4) to Apple Inc. Additionally, the sponsor noted the change in trade name from (b) (4) App to Irregular Rhythm Notification Feature. This amendment was logged in while the file was undergoing management review and is not reflected in the lead reviewer's memo.

The purpose of this memo is to document the Division's management recommendation that the De Novo be GRANTED (GRNT).

II. REGULATORY HISTORY

The lead reviewer's memo documents a thorough and thoughtful assessment of the regulatory history and previous interactions with the sponsor regarding the App under review.

Based on CDRH policy, the Apple Watch is not considered within scope of this review given that there are no medical claims being proposed for the Watch. The Watch and the iPhone are considered general purpose computing devices and are not subject to FDA review. The Watch acquires an electrical signal from contact with the user, but the electrical signal itself does not have a medical claim. However, the App that receives the electrical signal from the Watch PPG sensor and subsequently analyzes the signal to identify irregular heart rhythms suggestive of AF does meet the definition of a device. Therefore, the App is subject to FDA regulatory review and oversight.

III. INDICATIONS FOR USE

The sponsor has agreed to the following indications for use based on feedback from the FDA team:

> The Irregular Rhythm Notification Feature is a software-only mobile medical application that is intended to be used with the Apple Watch. The feature analyzes pulse rate data to identify episodes of irregular heart rhythms suggestive of atrial fibrillation (AFib) and provides a notification to the user. The feature is intended for over-the-counter (OTC) use. It is not intended to provide a notification on every episode of irregular rhythm suggestive of AFib and the absence of a notification is not intended to indicate no disease process is present; rather the feature is intended to opportunistically surface a notification of possible AFib when sufficient data are available for analysis. These data are only captured when the user is still. Along with the user's risk factors, the feature can be used to supplement the decision for AFib screening. The feature is not intended to replace traditional methods of diagnosis or treatment.
>
> The feature has not been tested for and is not intended for use in people under 22 years of age. It is also not intended for use in individuals previously diagnosed with AFib.

IV. REVIEW

The lead reviewer and his team have performed a rigorous scientific review and have concluded that the information provided in the De Novo submission and through subsequent interactions is not sufficient to establish a reasonable assurance of safety and effectiveness for the App for its intended use. At the conclusion of the review, the following deficiencies were identified by the review team:

<u>Statistical</u>

(b) (4)

[redacted]

(b) (4)

Management Review Comments: (b) (4)

I agree with (b) (4) ***conclusions and I believe this deficiency has been addressed.***

(b) (4)

(b) (4)

Management Review Comments: (b) (4)

This deficiency has been adequately addressed.

Software, Cybersecurity and Interoperability

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

Management Review Comments: ***This deficiency has been addressed by the sponsor, as detailed in the software consulting review memo completed by Linda Ricci on September 8, 2018. As discussed in Ms. Ricci's memo, while the software documentation was not ideal, it was minimally acceptable and supports the proposed App.***

(b) (4)

(b) (4)

(b) (4)

<u>Management Review Comments:</u> This deficiency has been addressed by the sponsor, as detailed in the software consulting review memo completed by Linda Ricci on September 8, 2018. As discussed in Ms. Ricci's memo, while the software documentation was not ideal, it was minimally acceptable and supports the proposed App.

(b) (4)

(b) (4)

Management Review Comments: ***This deficiency has been addressed by the sponsor, as detailed in the software consulting review memo completed by Linda Ricci on September 8, 2018. As discussed in Ms. Ricci's memo, while the software documentation was not ideal, it was minimally acceptable and supports the proposed App.***

Performance Testing

(b) (4)

(b) (4)

[redacted]

Management Review Comments (b) (4)

[redacted]

This deficiency has been adequately addressed.

(b) (4)

[redacted]

Management Review Comments: (b) (4)

[redacted]

This deficiency is considered resolved.

(b) (4)

[redacted]

(b) (4)

[redacted]

Management Review Comments: (b) (4)

[redacted]

I believe this deficiency has been adequately addressed.

(b) (4)

[redacted]

(b) (4)

Management Review Comments: ***While I agree that the sponsor's software documentation is not ideal, it is considered minimally acceptable as noted in Ms. Ricci's software consulting review memo. Of note, the sponsor explained during a teleconference on August 29, 2018 how the software requirements specification (SRS) and design document, when considered together, provide adequate information. I believe this deficiency has been adequately addressed.***

(b) (4)

Management Review Comments: (b) (4)

hile the sponsor's documentation is not ideal, I believe the response is adequate given the overall risk of the device. No additional information is needed, and this deficiency has been adequately addressed.

V. BENEFIT-RISK ASSESSMENT

(b) (4)

(b) (4)

[redacted]

Management Review Comments: (b) (4) ***performed an excellent clinical review of the proposed App and provided a thoughtful assessment of the benefits and risks. I agree with his overall assessment that the benefits outweigh the risks for the intended user population.***

(b) (4)

[redacted]

VI. FINAL RECOMMENDATION

An extremely comprehensive and thorough review has been performed by Mr. Erdit Gremi and his FDA review team. I believe, however, that the remaining deficiencies cited by Mr. Gremi have been adequately addressed.

As such, I have concluded that the information provided by the sponsor demonstrates that there is a reasonable assurance of safety and effectiveness for the device for its intended use. I believe the benefits of the Irregular Rhythm Notification Feature outweigh the risks and I recommend this De Novo be granted.

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

U.S. FOOD & DRUG ADMINISTRATION

Food and Drug Administration
CDRH/ODE/DCD/CDDB
WO66 RM1102
10903 New Hampshire Ave
Silver Spring, MD 20993-0002
240-402-3910

De Novo Review

Date: September 6, 2018

Reviewer: Erdit Gremi

Subject: Direct De Novo # DEN180042

Applicant: (b) (4)

Device Trade Name: (b) (4) App

Contact Name: Donna-Bea Tillman

Contact Title: Senior Consultant

Correspondent Firm: Biologics Consulting Group

Phone: (410) 531-6542 **Email:** dtillman@biologicsconsulting.com

Received Date: 08/09/2018

Due Date: 08/24/2018

Reg #:

Reg Name:

Pro Code(s):

Class: [Choose] **510k Exempt Yes/No** [Choose]

Post-NSE 510k :

Submission #	Pro Code	Device Trade Name	Applicant

Recommendation

I recommend that the De Novo request for the (b) (4) App is declined (DEND)

Review Summary

This de novo submission is for an OTC software only device which analyzes PPG data collected from the Apple Watch Series 1, 2, 3, and 4 platforms and produces a notification of an irregular heart rhythm consistent with Atrial Fibrillation.(b) (4) In this memo "Apple" (meaning Apple, Inc.) and (b) (4) (meaning (b) (4)) are used interchangeably, both indicating the sponsor of this submission.

In support of the submission, the sponsor has included details of a clinical trial using the (b) (4) software which demonstrates, the performance in a population, software documentation to demonstrate the testing and hazard mitigations in the device, a human factors study, labeling and a description of the subject device.

After extensive review of the sponsors documentation as well as almost daily interactive review done with the sponsor on a pilot de novo timeline, there are some concerns that remain outstanding for the subject device. The outstanding issues include concerns with the performance of the device in the intended use population instead of the study population that was included in the clinical study used to support the submission as well as a still unofficial interim analysis of a larger clinical study from which that sub study was derived. The conclusions drawn from these trials as well as the statistical analysis of these data continue to remain deficient. Additionally, the manner in which the sponsor has provided a hazard analysis, the mitigations that have been included in that analysis for various hazards, the requirements in the software for mitigating those hazards, and the testing that was conducted to validate that those requirements remains deficient. Finally, the performance of the device algorithm and the specificity of software and platform requirements to ensure that the performance can remain safe and effective across all compatible platform versions as well as be translatable and testable in future versions remains deficient.

These deficiencies are not insurmountable and would normally require a detailed revision from the sponsor to fully identify the breadth and depth of hazards posed by the sponsor device, testable requirements that need to exist in order to mitigate those hazards and testing to demonstrate a passing condition throughout the possible foreseeable use

conditions. Additionally, the sponsor could simply provide final clinical trial data from the ongoing trial set to conclude in early 2019 to support the use of the device in the intended use population instead of the sub-study data which has extensive statistical concerns. It is the opinion of the Lead Reviewer that these concerns be communicated to the sponsor through a traditional AINN Letter so that the sponsor can have time to address the concerns and the FDA can review them. However, the Lead Reviewer has been directed to make a Final Decision Recommendation to either Grant or Decline the de novo. Due to the deficiencies that remain outstanding, the file cannot receive a granting recommendation at this time.

Review Team

Lead Reviewer	Erdit Gremi (CDRH/ODE/DCD/CDDB)
Software Consult	Natalie Yarkony (CDRH/ODE/DCD/CDDB)
Algorithm Consult	Loriano Galeotti (CDRH/ODE/DCD/CDDB)
Human Factors Consult	Kimberly Kontson (CDRH/OSEL/DBP)
Clinical Consult	Kan Fang (CDRH/ODE/DCD/CEDB)
Statistical Consult	Xuan Ye (CDRH/OSB/DBS/DSB1)
Statistical Consult	Arkendra De (CDRH/OSB/DBS/DSB1)

The review of the interactive deficiencies which were sent to the sponsor upon initial review of the de novo submission is included in each subsection of this memo and is highlighted in blue.

I. Background, Submission Summary and De Novo Eligibility

De Novo Eligibility	
What is the sponsor's recommended classification for the subject device?	Class II
Do you wish to conduct a De Novo eligibility review for this device (required for originals)?	Undo No

De Novo Eligibility

The sponsor provided an evaluation of possible predicates for this device which is similar to the search conducted on an FDA database for similar devices. The results of that predicates search are as follows:

Device	Indication for Use	Comparison
K110374, Medicore Max Plus System	Provides noninvasive measurement of pulse waveform and heart rate by photoelectric plethysmography. Indicated for use in hospitals, health care clinics, and physicians' offices.	While using PPG technology, the intended use is different. The (b) (4) App is intended for identifying irregular heart rhythms, while this device is cleared for measuring waveform and heart rate. This device is also cleared for Rx, not OTC, use.
K142743, AliveCor Kardia Mobile	Intended to record, store and transfer single-channel electrocardiogram (ECG) rhythms. It also displays ECG rhythms and detects the presence of atrial fibrillation and normal sinus rhythm (when prescribed or used under the care of a physician).	This device uses ECG, rather than PPG technology. It is also cleared for a combination Rx/OTC use, rather than solely OTC.
K151269, LifeWatch ECG Mini System Continuous ECG Monitor and Arrhythmia Detector	Intended for use by patients who experience transient symptoms that may suggest cardiac arrhythmia. The device continuously monitors patient ECG, automatically generates an alarm triggered by an arrhythmia detection algorithm, or generates an alarm manually triggered by the patient, and transmits the recorded data to a monitoring center, which provides the ECG data to the medical practitioner for evaluation.	This device uses ECG rather than PPG technology, and is intended for Rx rather than OTC use.

K151330, Microlife Wrist Watch Blood Pressure Monitor	Intended to measure the blood pressure and pulse rate by using a non-invasive oscillometric technique in which an inflatable cuff is wrapped around the wrist. The device detects the appearance of irregular heartbeat during measurement and gives a warning signal with the reading once the irregular heartbeat is detected.	This device does not use PPG technology, and is primarily intended for use as a blood pressure monitor.
K163045, Omron Wrist Blood Pressure Monitor	The device is a digital monitor intended for use in measuring blood pressure and pulse rate. The device detects the appearance of irregular heartbeats during measurement and gives a warning signal with readings.	This device does not use PPG technology, and is primarily intended for use as a blood pressure monitor.
K171816, AliveCor Kardia Band System	Intended to record, store and transfer single-channel electrocardiogram (ECG) rhythms. It also displays ECG rhythms and detects the presence of atrial fibrillation and normal sinus rhythm (when prescribed or used under the care of a physician). The Kardia Band System is intended for use by healthcare professionals, adult patients with known or suspected heart conditions and health conscious individuals.	This device uses ECG, rather than PPG technology. It is also cleared for a combination Rx/OTC use, rather than solely OTC.

There does not appear to be a suitable predicate device for the (b) (4) App. The devices that use PPG technology are not intended for use to identify irregular heart rhythms, and the devices that do detect irregular heart rhythms do not use PPG technology. There are no PPG devices that are intended for the continuous monitoring of pulse rate for determining irregular heart rhythm or Atrial Fibrillation. Therefore, the (b) (4) App is different from currently marketed devices, and can properly be regulated through the de novo pathway.

TPLC Information

(b) (4)

(b) (4)

(b) (4)

II. Device/System Description

Is this device eligible for De Novo?	Yes	Undo

Device Description Information Red = Inadequate or Unanswered Yellow = Marked

Device is life-supporting or sustaining: No

There are direct/indirect patient contacting components: No

Device uses software/firmware: Yes

- **Device is or contains Digital Health technology:** Yes
- **Connection Types:** Cloud, Network, Wireless

Device or component needs sterilization: No

Use/Reuse information: Reusable single patient use

Device Description Information	Red = Inadequate or Unanswered	Yellow = Marked
Environments of Use: Home		
Combination Product Type: N - Not a Part 3 Combination Product		
The Device/System is electrical: Yes, it is battery powered Only		
• **Wireless Technology is used:** Yes		
Device Attributes		
Nanotechnology present: No		
Companion Diagnostic: No		
Medical Counter Measures: No		

(b) (4)

(b) (4)

[redacted]

Reviewer Recommendation

The Device Description, including technology description, is acceptable.

III. Indications for Use

Indications for Use

Subject

De Novo #: DEN180042 Rx/OTC: OTC

Intended Population	Adults Only	Adults and Pediatrics	Transitional Adolescent A	Transitional Adolescent B	Adolescent	Child	Infant	Neonate/ Newborn
Yes	☒	☐	☐	☐	☐	☐	☐	☐
No	☐	☒	☒	☒	☒	☒	☒	☒
Unknown	☐	☐	☐	☐	☐	☐	☐	☐

Indications for Use: (b)(4) Draft

[redacted]

(b) (4)

[redacted]

Reviewer Recommendation

The Indications for Use are acceptable.

IV. Labeling

Labeling Review Needed?	Yes	Undo
Usability Consult Needed?	Yes	Undo

Labeling Information	Red = Inadequate or Unanswered	Yellow = Marked
Prescription statement included: Inapplicable		
Adequate OTC instructions: No		
Indications for Use are consistent in submission: Yes		
Appropriate Contraindications, Warnings, Precautions & Adverse Events: No		
Instructions in accordance with guidance: Inapplicable		
Appropriate labeling inside device: Inapplicable		
Appropriate labeling outside device: Inapplicable		
Appropriate instructions for use labeling: Yes		
Appropriate Home Use information: Yes		
MR Status according to labeling: THIS QUESTION WAS NOT ANSWERED		

(b) (4)

[redacted]

(b) (4)

Reviewer Recommendation

The Labeling is acceptable.

V. Reprocessing, Sterilization, and Shelf-Life

Reviewer Recommendation

Cleaning, Sterilization, Shelf-Life and Reuse descriptions are not applicable as (b) (4) is a software only device.

VI. Biocompatibility

Reviewer Recommendation

The Biocompatibility information is not applicable as (b) (4) is a software only device.

VII. Software/Firmware & Cybersecurity/Interoperability

Software Review Needed?	Yes	No	Cybersecurity/Interoperability Review Needed?	Yes	No
Software Consult Needed?	Yes	No	Cybersecurity/Interoperability Consult Needed?	Yes	No

(b) (4)

(b) (4)

(b) (4)

Reviewer Recommendation

The Software is not acceptable.

VIII. EMC, Wireless, Electrical, Mechanical and Thermal Safety & Risk Analysis

EMC Review Needed?	Yes	No	Wireless Review Needed?	Yes	No
EMC Consult Needed?	Yes	No	Wireless Consult Needed?	Yes	No

Reviewer Recommendation

The EMC, Wireless, EMT and Risk Analysis are not applicable as (b) (4) is a software only device.

IX. Performance Testing

A Bench Testing

(b) (4)

B Animal Testing

None

C Clinical Testing

(b) (4)

(b) (4)

(b) (4)

[redacted]

Reviewer Recommendation

The Performance Testing is not acceptable.

X. Special/General Controls Information

Table 1: Identified Risks to Health and Mitigation Measures

Identified Risk	Mitigation Measures
Poor quality PPG signal resulting in failure to detect irregular heart rhythms	Clinical performance testing Human factors testing
Misinterpretation and/or over-reliance on device output, leading to: • Failure to seek treatment despite acute symptoms "e.g. fluttering sensation in their chest, lightheadedness, and irregular pulse)	Clinical performance testing Human factors testing Labeling

• Discontinuation from treatment for chronic heart condition	
False negative resulting in failure to detect irregular heart rhythms and delay of further evaluation or treatment	Clinical performance testing Software verification, validation, and hazard analysis Non-clinical performance testing
False positive resulting in additional unnecessary medical procedures and patient anxiety	Clinical performance testing Software verification, validation, and hazard analysis Non-clinical performance testing Postmarket surveillance
Failure to identify correct population and condition	Label comprehension and self-selection study

Special Controls (Class II Only)

The special controls are as follows:

1. Clinical data must demonstrate the performance characteristics of the diagnostic algorithm .
2. Software verification, validation, and hazard analysis must be performed. Documentation must include a characterization of the technical specifications of the software, including the diagnostic algorithm and its inputs and outputs.
3. Non-clinical performance testing must demonstrate that the device performs as intended under anticipated conditions of use.
4. A label comprehension and self-selection performance evaluation must demonstrate that the intended OTC users can understand the device labeling and correctly self-identify within the intended use population.
5. Human factors and usability testing must demonstrate that the layman can correctly interpret the device output and seek appropriate care when necessary based solely on reading the device labeling.
6. Postmarket surveillance must be conducted and completed in accordance with an FDA-agreed upon protocol.
7. Labeling must include:
    a. Hardware platform and operating system requirements;
    b. Situations in which the device may not operate at an expected performance level;
    c. A description of what the device measures and outputs to the user; and
    d. Guidance on interpretation of any diagnostic results.

XI. Classification Discussion

This section must be completed only when granting the De Novo. However, pertinent information (e.g. discussion of sponsor's proposed classification) can be included at any time.

Regulation Identification

FDA identifies this type of device as:

Exemption from 510(k)

Reviewer Recommendation

The Classification Discussion, Identification and Exemption from 510(k) are **[not]** acceptable.

XII. Benefit/Risk Assessment

(b) (4)

[redacted]

(b) (4)

[redacted]

a. Patient Perspectives

This was not conducted.

XIII. Summary of Meetings

There have been extensive interactions with the sponsor in order to address the concerns that were identified during the review. (b) (4)

[redacted] The meeting minutes of the teleconference are located in DocMan for that Q-Sub.

(b) (4)

[redacted]

(b) (4) The meeting minutes of the teleconference are located in DocMan for that Q-Sub Supplement.

This de novo submission was received by email on August 7th, 2018 and officially received (by the Document Control Center) on August 9, 2018. On August 14th, 2017, the sponsor held a teleconference with FDA where they provided a summary explanation of the clinical report that was provided in the de novo. The meeting minutes from that call are included in DocMan. FDA provided interactive questions to the sponsor first on August 14th, 2017 to present FDA concerns regarding the applicability of the clinical data results to the general population as well as propose a design change which would serve as a solution to the concern. The August 14th email is included in DocMan. There have also been daily calls with the sponsor to interactively communicate concerns and receive feedback.

A detailed account of the interactive emails that were sent to the sponsor is included in DEN180042.LeadMemo.AppendixA.

XIV. References

none

XV. Original Major Deficiencies

Statistical

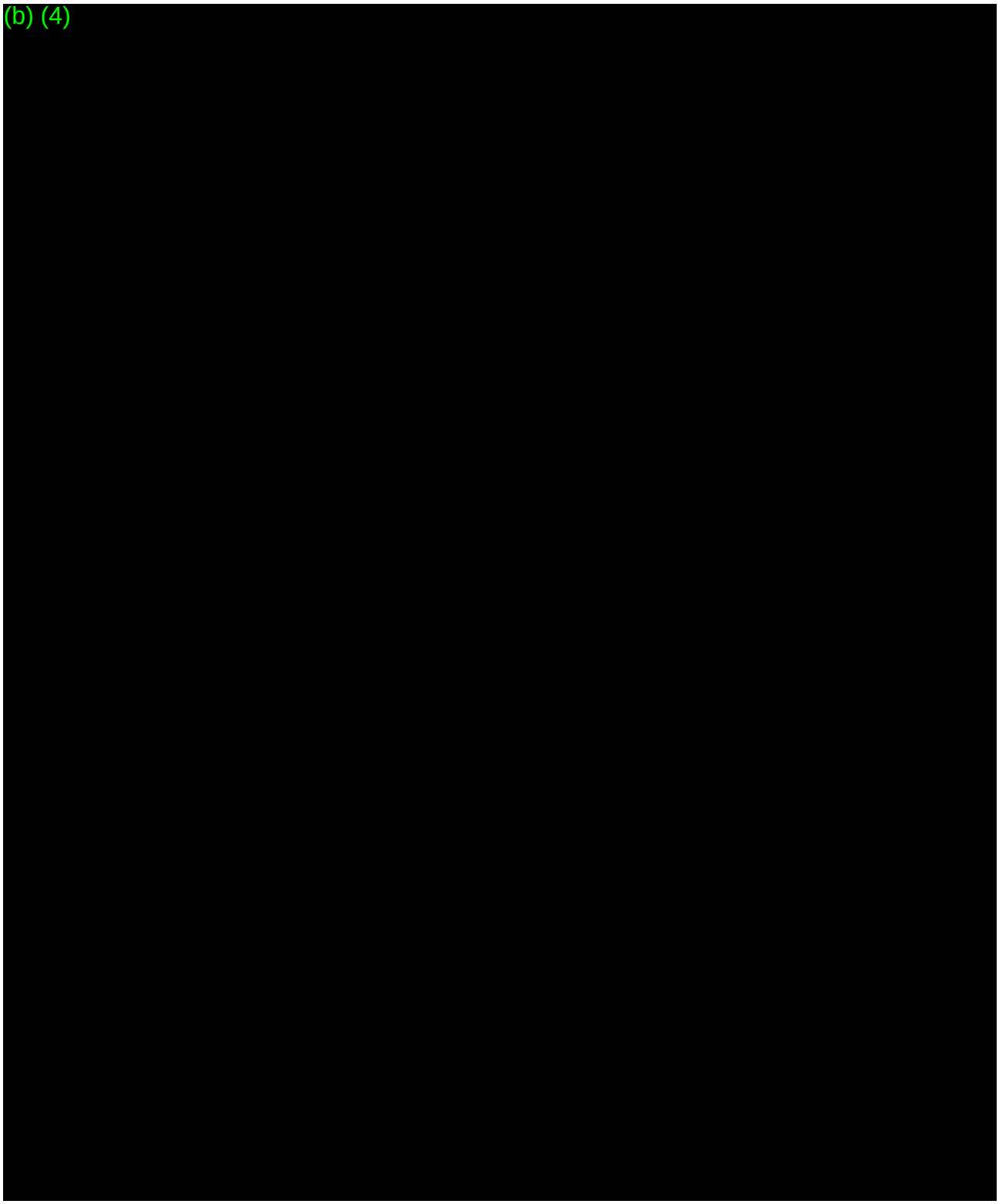
(b) (4)

(b) (4)

Please address these concerns regarding the estimated performance of the subject device on the intended use population.

Software, Cybersecurity and Interoperability

(b) (4)



(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

Performance Testing

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

XVI. Original Minor Deficiencies

None

XVII. Original Additional Considerations

None

XVIII. Contact History

A detailed account of the interactive emails that were sent to the sponsor is included in DEN180042.LeadMemo.AppendixA.

Digital Signature Concurrence Table (Doc#: 04025.01.11)	
Reviewer Sign-Off	Erdit Gremi -S 2018.09.08 13:11:20 -04'00'

ODE (OPEQ Pilot OHT1 - OHT6): Concurrence needed by DHT Assistant Director, OHT Director, ORP, and RPG Associate Director; consult the ODE De Novo SOP for additional information.

NOTE: Request a new procode via CTS if you didn't have a procode from the NSE'd 510k.

(b) (4)
% Donna-Bea Tillman
Senior Consultant
Biologics Consulting Group
1555 King St, Suite 300
Alexandria, Virginia 22314

Re: DEN180042
Trade/Device Name: (b) (4) App
Regulatory Class: Class III
Product Code: n/a
Dated: August 8, 2018
Received: August 9, 2018

Dear Donna-Bea Tillman:

The Center for Devices and Radiological Health (CDRH) of the Food and Drug Administration (FDA) has completed its review of your De Novo request for classification of the (b) (4) App with the following indications:

(b)(4) Draft

Based upon the information within your De Novo request, FDA concludes that you have not demonstrated that this device meets the criteria under section 513(a)(1) of the Federal Food, Drug and Cosmetic Act (21 U.S.C. 360c(a)(1) (the FD&C Act) for classification into class I or II. This decision is based on the fact that

you have not provided sufficient information to demonstrate that the probable benefits of the device outweigh its probable risks to health.

This order, therefore, declines your request and the device remains in class III (Premarket Approval).

In accordance with section 513(f)(1) of the FD&C Act (21 U.S.C. 360c(f)(1)), devices that were not in commercial distribution prior to May 28, 1976 (the date of enactment of the Medical Device Amendments of 1976 (the amendments)), generally referred to as postamendments devices, are classified automatically by statute into class III without any FDA rulemaking process. These devices remain in class III and require premarket approval, unless and until the device is classified or reclassified into class I or II or FDA issues an order finding the device to be substantially equivalent, in accordance with section 513(i) of the FD&C Act (21 U.S.C. 360c(i)), to a predicate device that does not require premarket approval. The agency determines whether new devices are substantially equivalent to previously marketed devices by means of premarket notification procedures in section 510(k) of the FD&C Act (21 U.S.C. 360(k)) and Part 807 of the FDA regulations (21 CFR 807).

Please note that section 513(f)(2) of the FD&C Act, also referred to as De Novo classification or Evaluation of Automatic Class III Designation, was amended by section 607 of the Food and Drug Administration Safety and Innovation Act (FDASIA) on July 9, 2012. This law provides two options for De Novo classification. First, any person who receives a "not substantially equivalent" (NSE) determination in response to a 510(k) for a device that has not been previously classified under the Act may request FDA to make a risk-based classification of the device under section 513(a)(1) of the Act. On December 13, 2016, the 21st Century Cures Act removed a requirement that a De Novo request be submitted within 30 days of receiving an NSE determination. Alternatively, any person who determines that there is no legally marketed device upon which to base a determination of substantial equivalence may request FDA to make a risk-based classification of the device under section 513(a)(1) of the Act without first submitting a 510(k).

On August 9, 2018, FDA received your De Novo requesting classification of the (b) (4) App. The request was submitted under section 513(f)(2) of the FD&C Act. In order to classify the (b) (4) App into class I or II, it is necessary that the proposed class have sufficient regulatory controls to provide reasonable assurance of the safety and effectiveness of the device for its intended use. After review of the information submitted in the request FDA has determined that the (b) (4) App, for the previously stated indications for use, cannot be classified in class I or II.

If you choose to submit a new direct De Novo request in response to this letter, please ensure that you have addressed all of the following concerns, and please cross-reference this submission as part of your new direct De Novo:

Statistical

(b) (4)

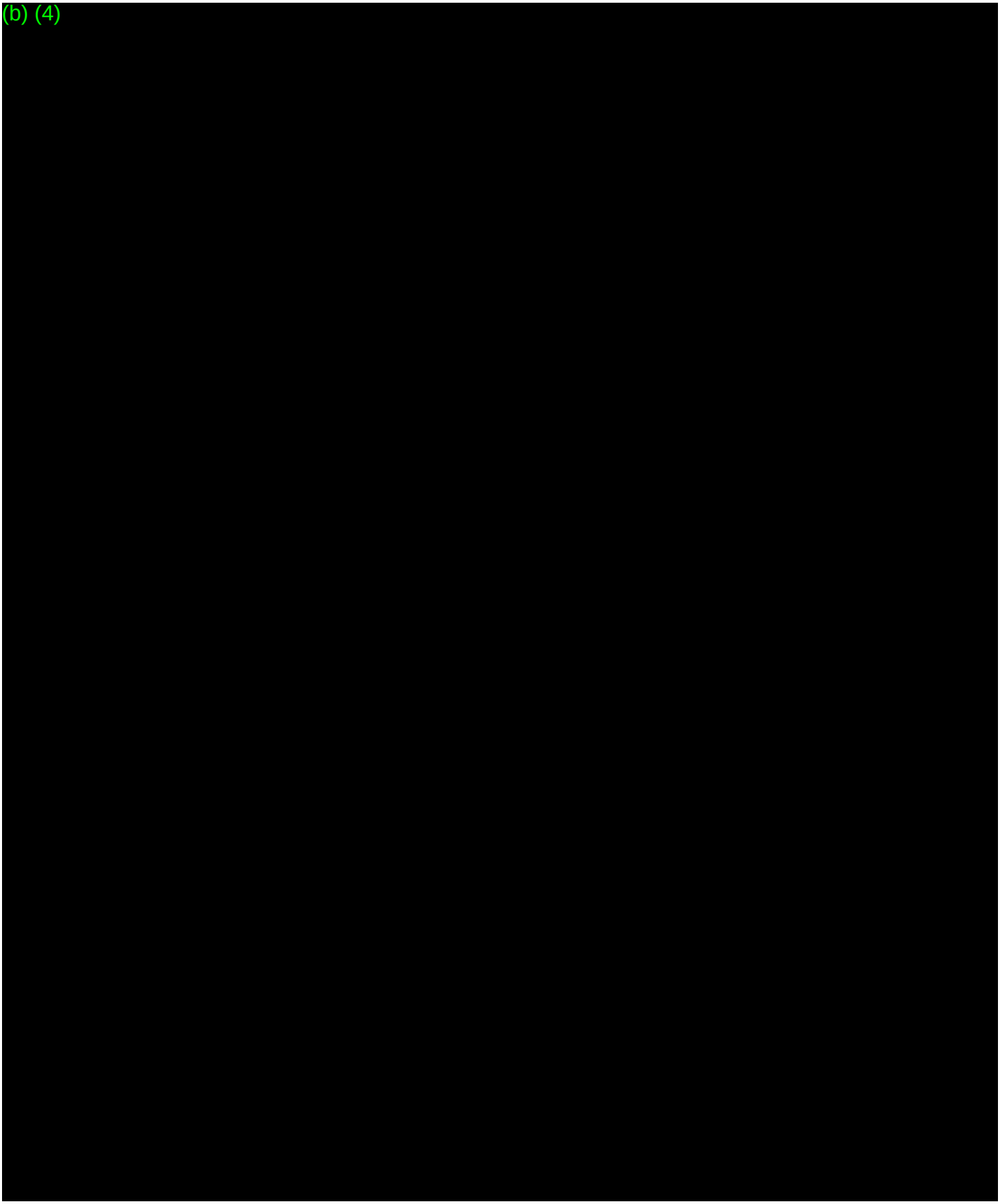
(b) (4)

(b) (4)

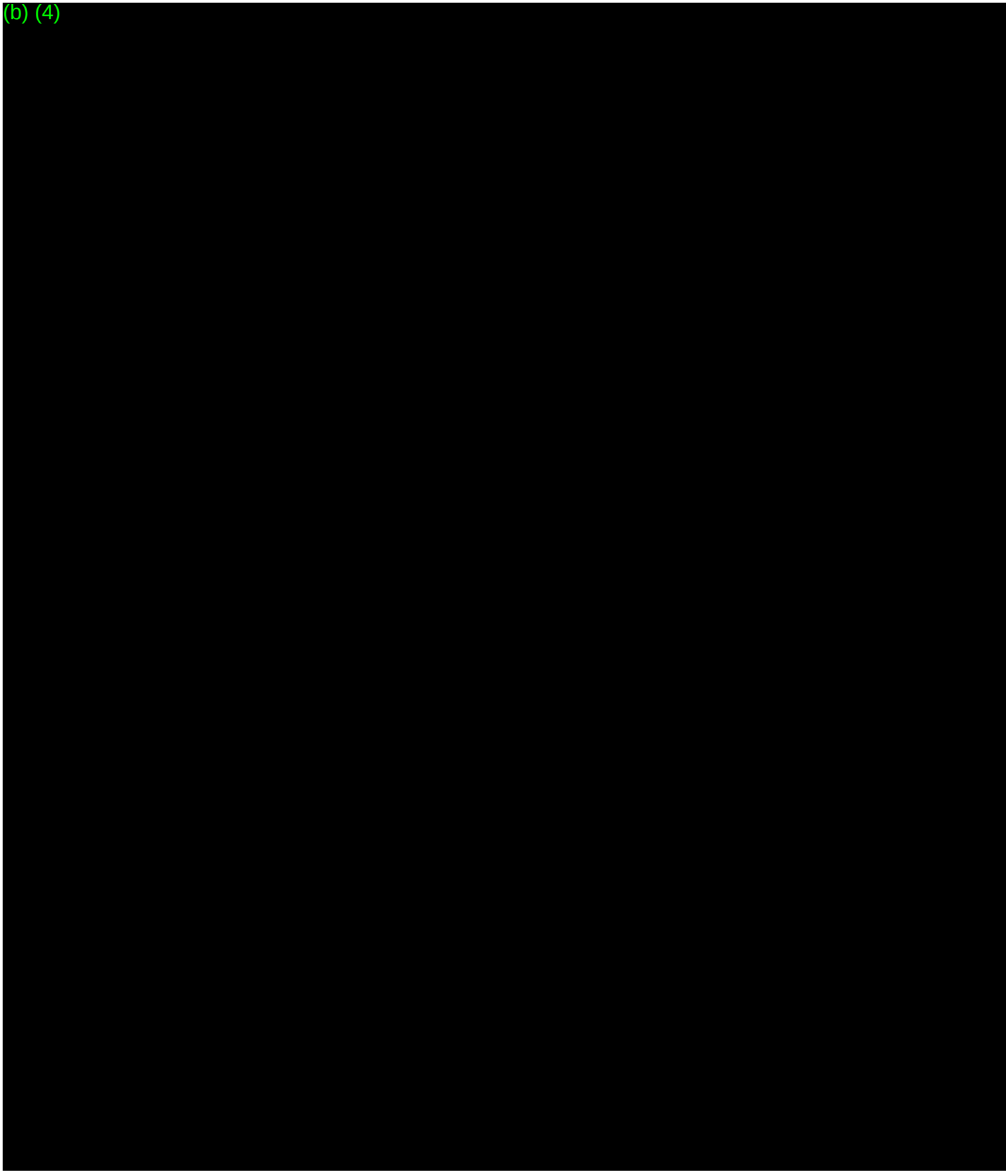
Software, Cybersecurity and Interoperability

(b) (4)

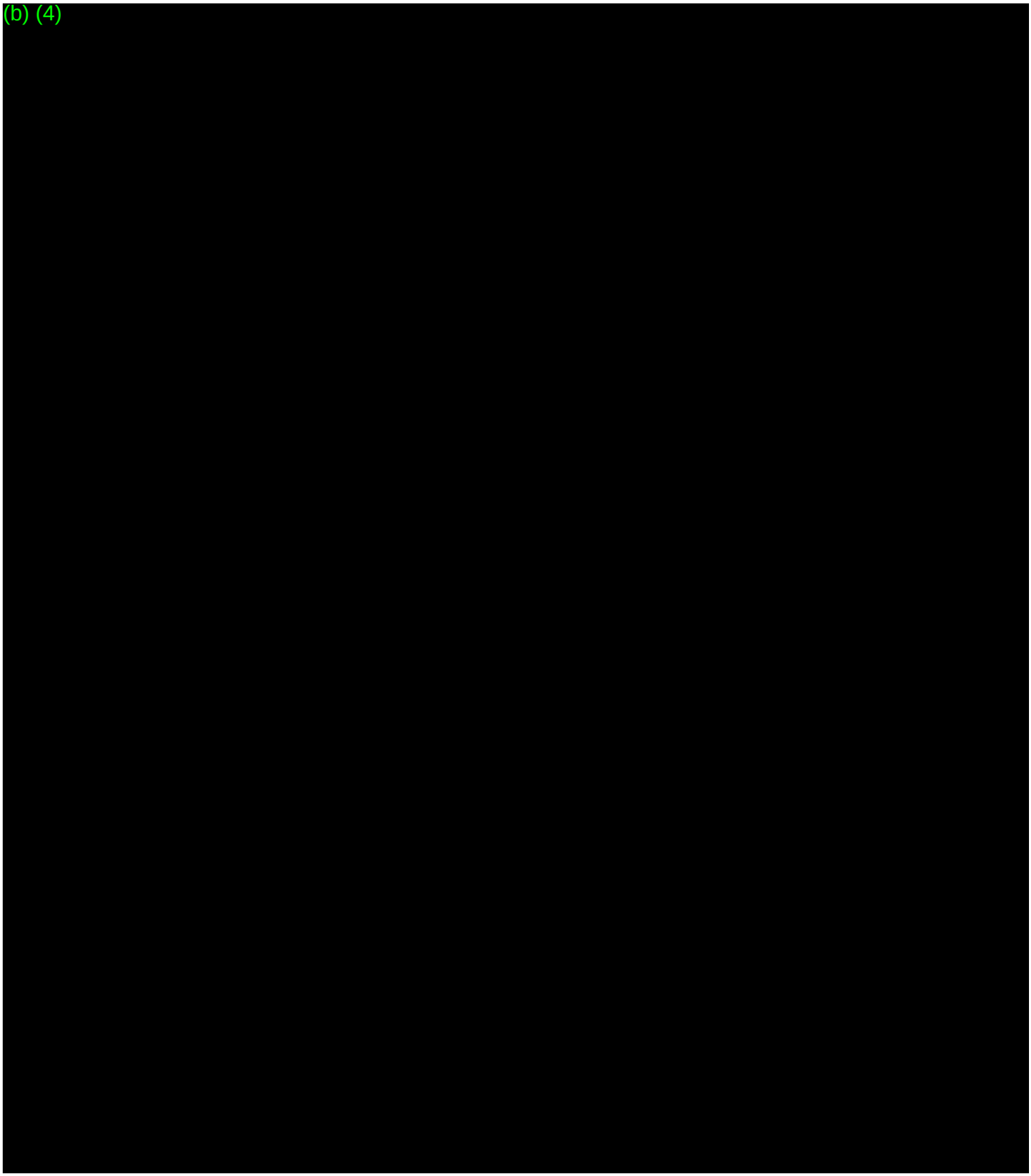
(b) (4)



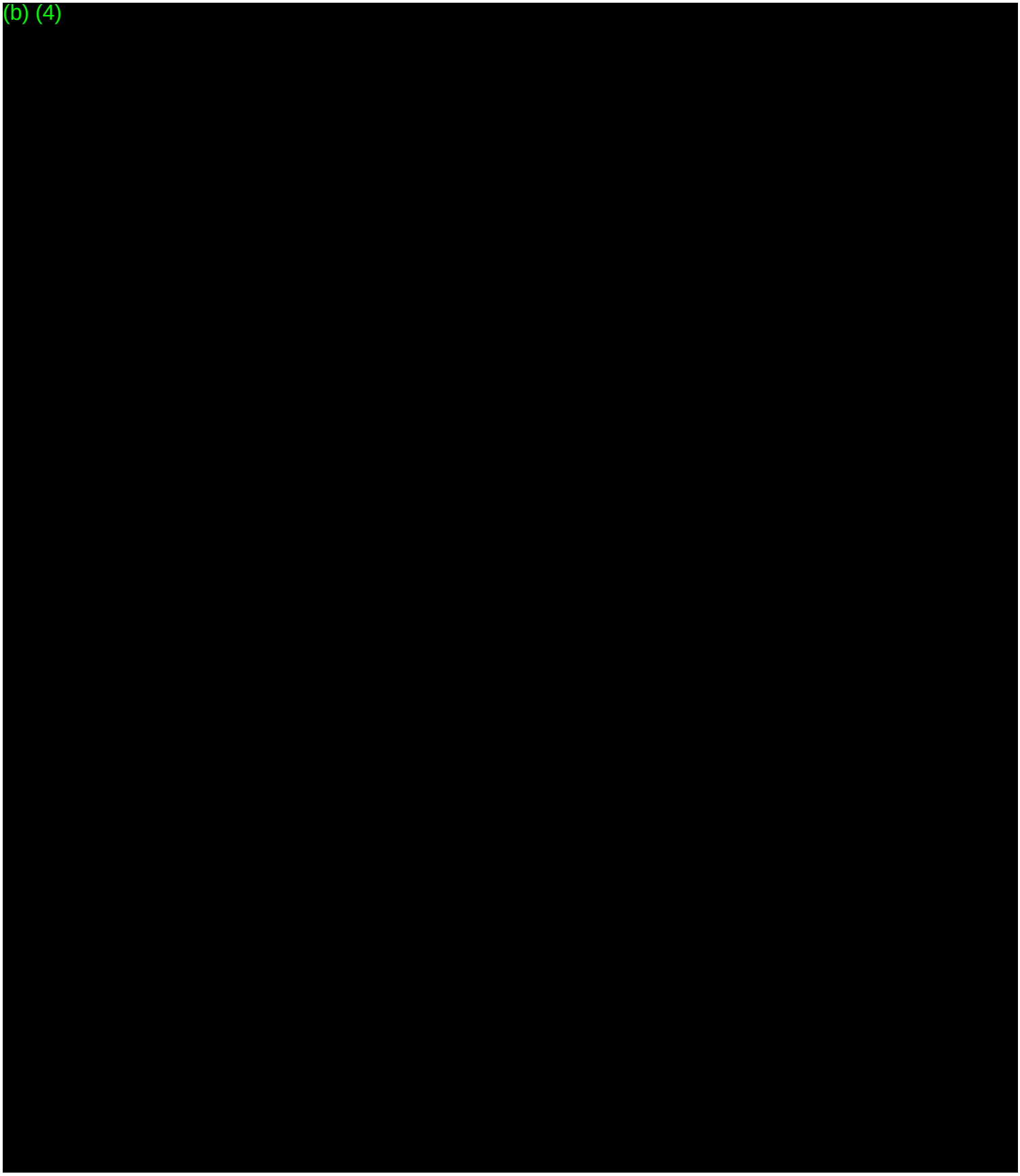
(b) (4)



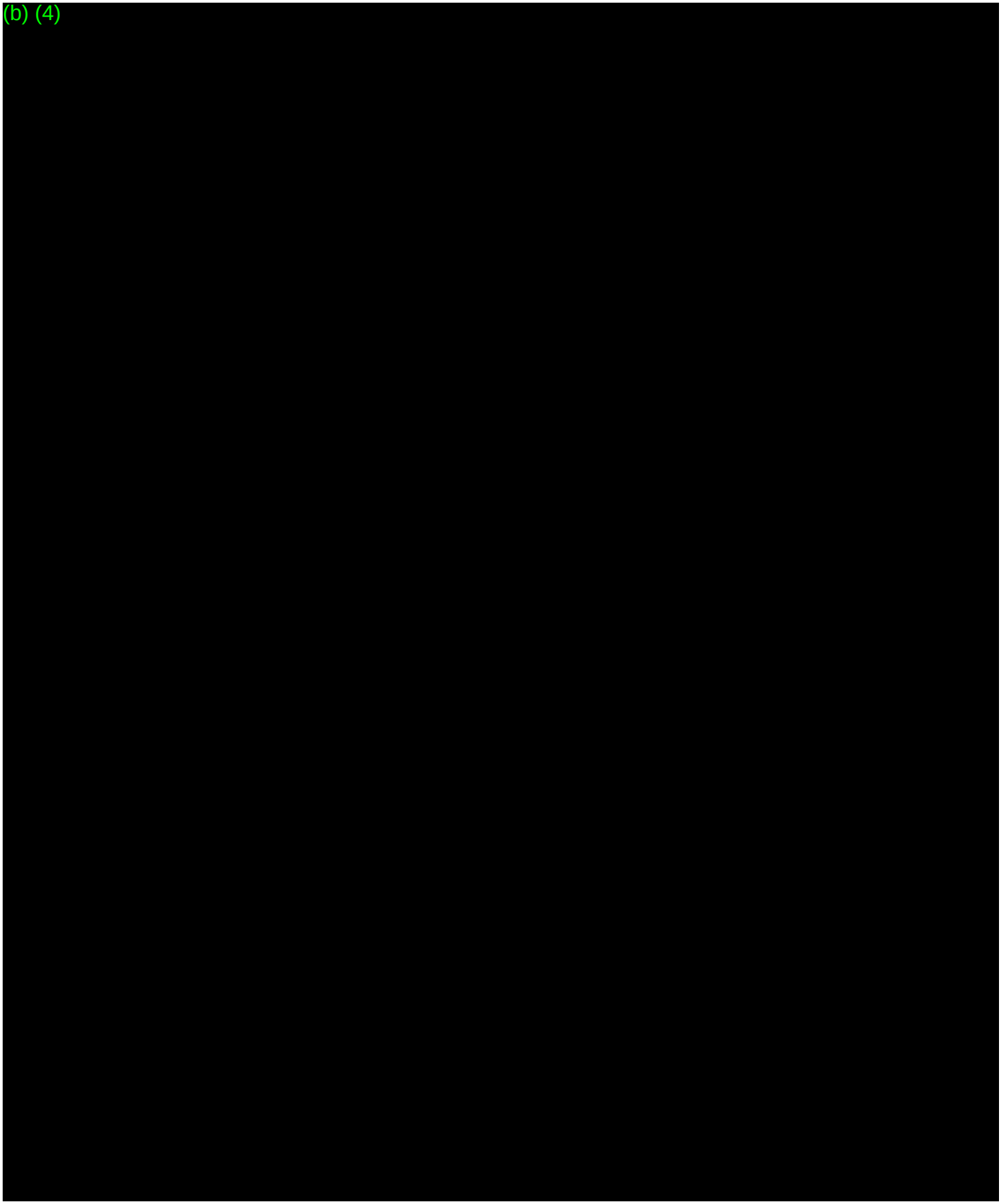
(b) (4)



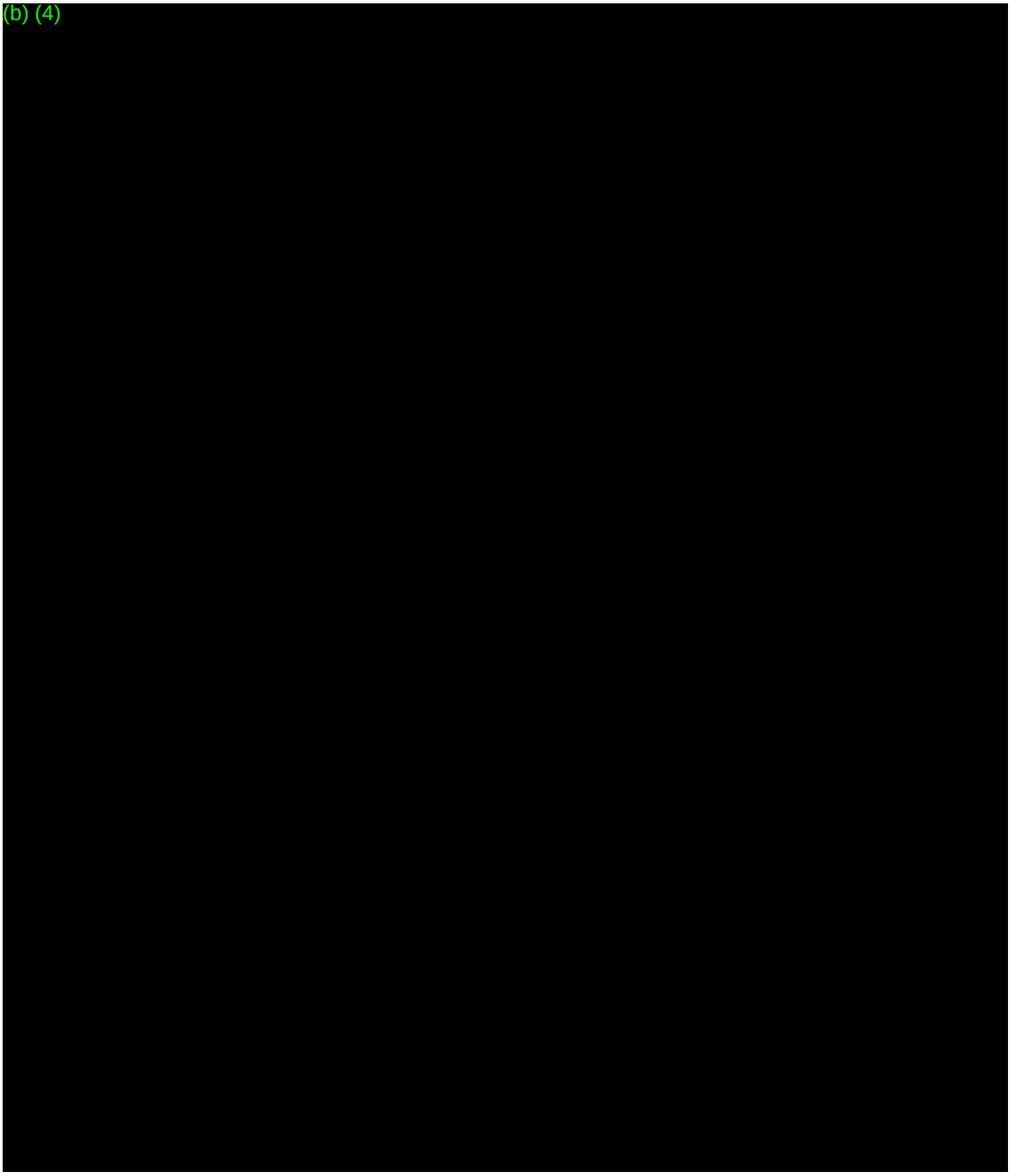
(b) (4)



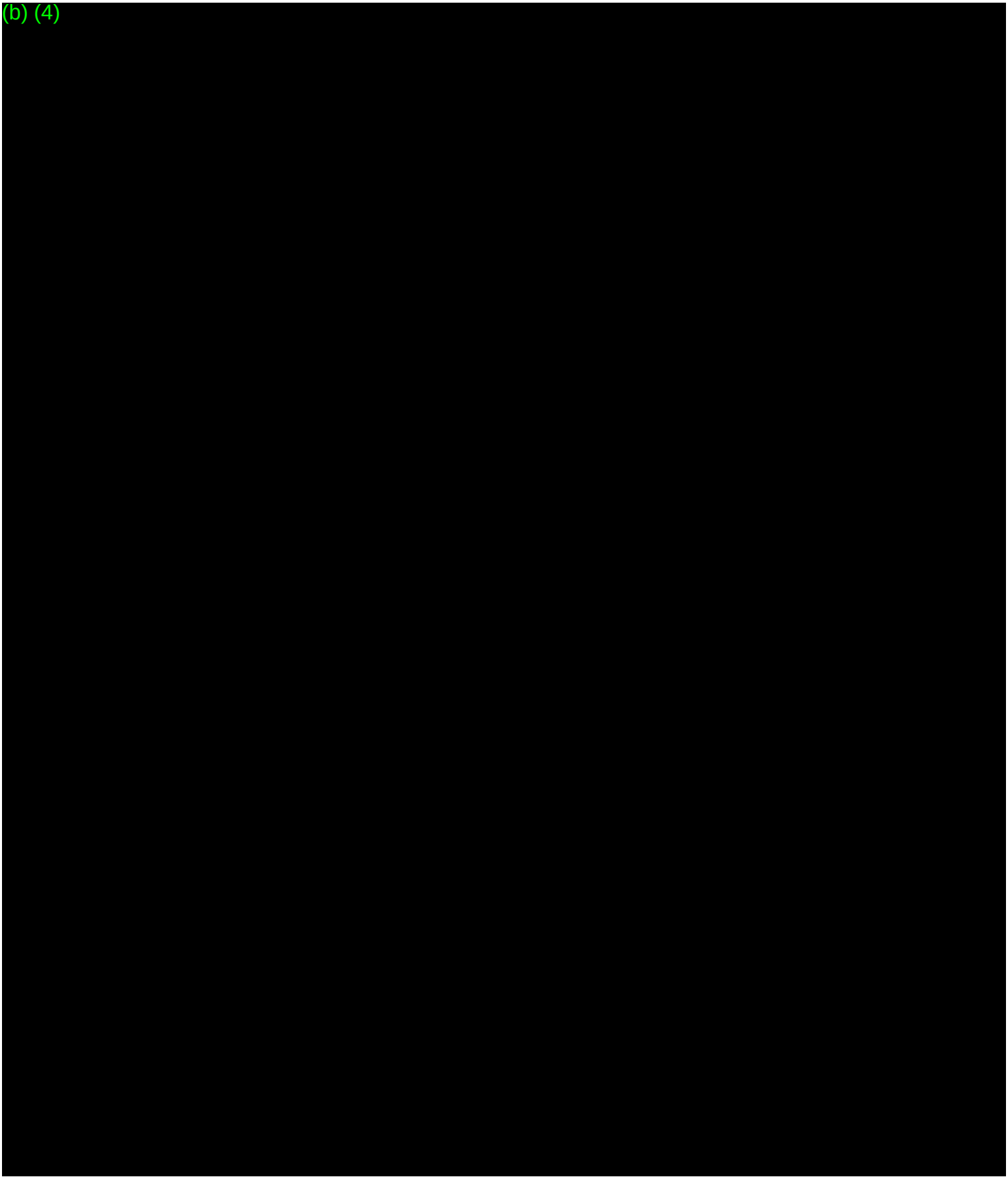
(b) (4)



(b) (4)

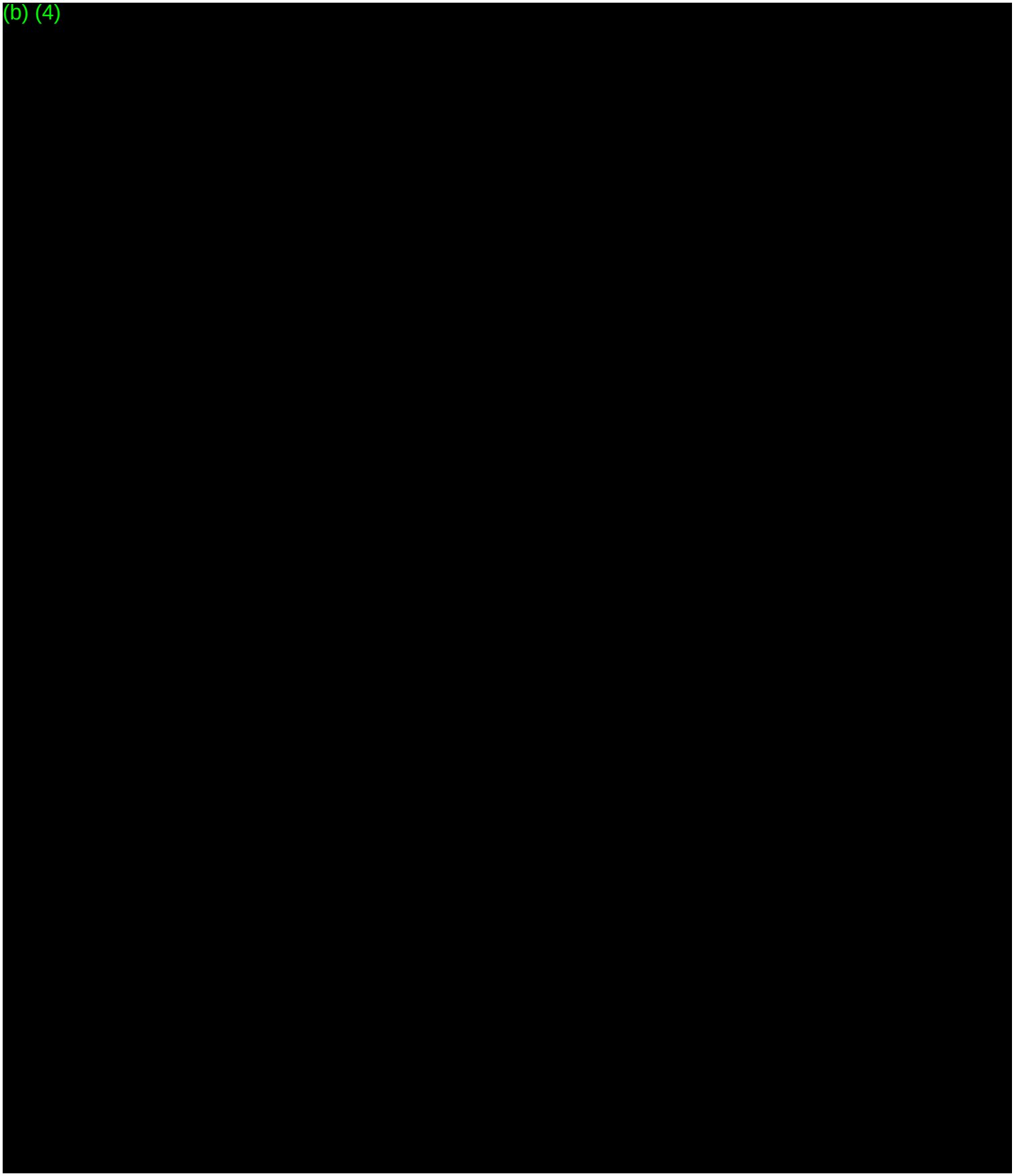


(b) (4)

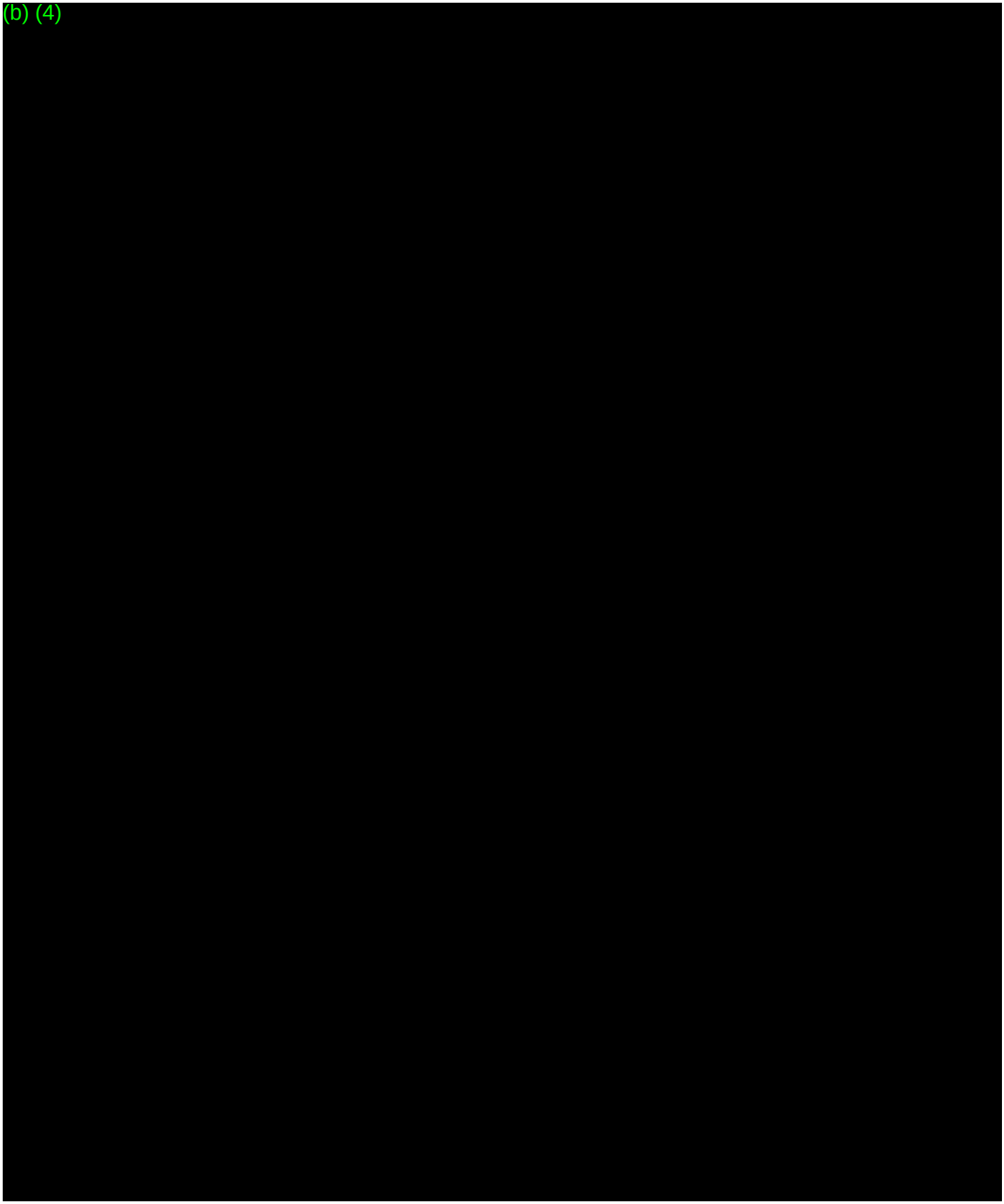


(b) (4)

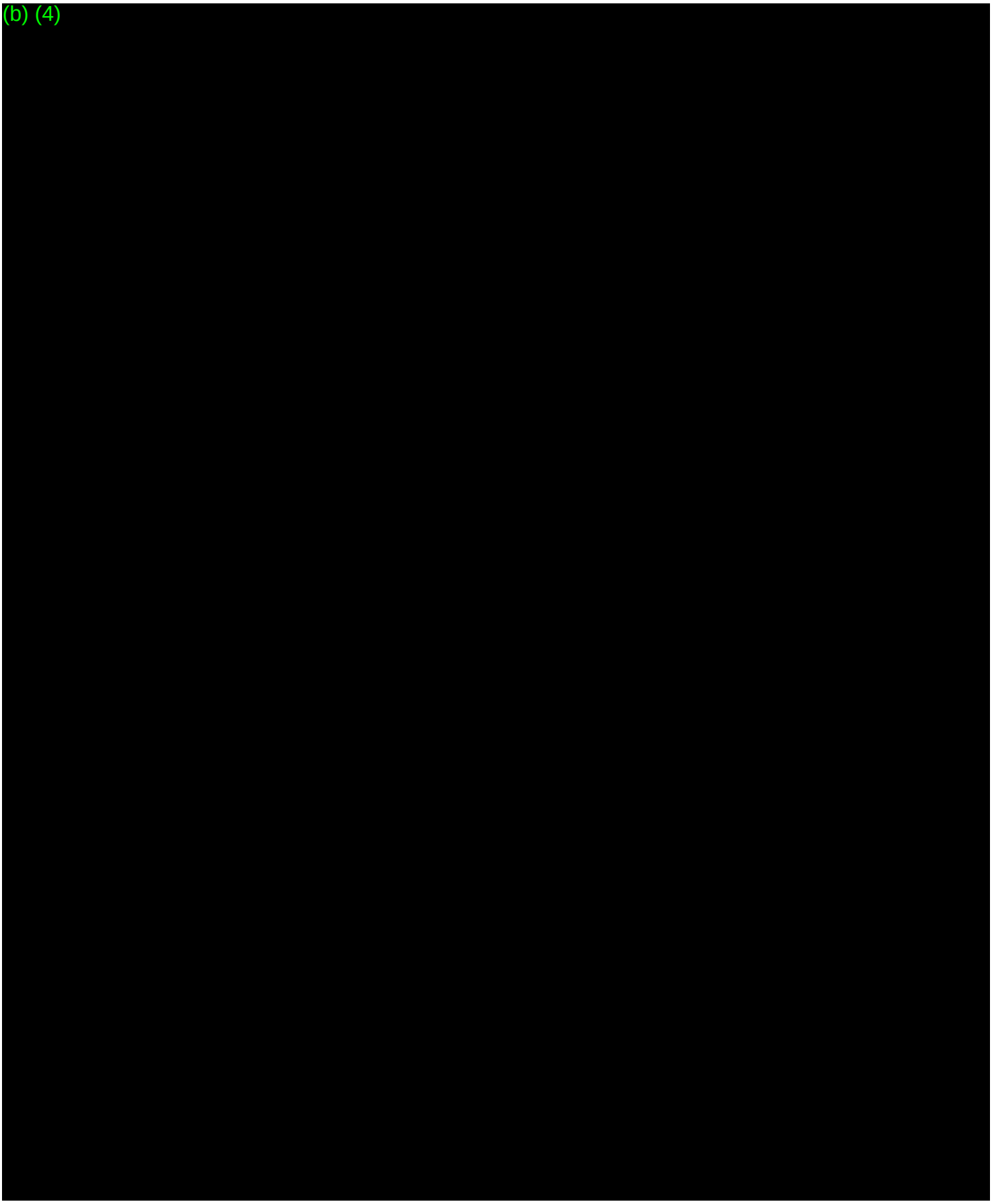
(b) (4)



(b) (4)



(b) (4)



(b) (4)

(b) (4)

We suggest that those considering the De Novo pathway, first submit a pre-submission so that FDA can engage in dialogue with the submitter to ensure that the device is appropriate for the De Novo process, and that any eventual De Novo submission contains the information necessary for FDA to complete a substantive review to determine whether general and/or special controls provide a reasonable assurance of safety and effectiveness of the device.

Further, in accordance with FDA's Guidance document regarding Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval and De Novo Classifications (http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm517504.pdf), FDA will make a Benefit-Risk assessment as part of its review. FDA recommends that you consider this guidance document in the preparation of any future premarket submission for this device. Further, as you formulate your submission, you may want to take into account the Questions to Consider in the Worksheet for Benefit-Risk Determinations (included as Appendix B in the guidance document); in particular, you may want to provide a summary of the type of benefit(s) of the device (as is queried in the 1st section of the worksheet).

Under section 501(f)(1)(B) of the FD&C Act (21 U.S.C. 351(f)(1)(B)), a device that is placed in class III under section 513(f) of the FD&C Act is adulterated and may not be introduced into commercial distribution, unless it has in effect an approved application for premarket approval under section 515 of the FD&C Act (21 U.S.C. 360e) or an investigational device exemption under section 520(g) of the FD&C Act (21 U.S.C. 360j(g)).

If you have any questions concerning this classification order, please contact Erdit Gremi at 240-402-3910.

Sincerely,

LETTER SHOULD BE DATED BEFORE SIGNING, AND MUST BE SIGNED OUT OF CTS ON THE DATE INDICATED ON THE LETTER.

Angela C. Krueger
Deputy Director, Engineering and Science Review
Office of Device Evaluation
Center for Devices and Radiological Health

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002

MEMORANDUM

DATE: September 8, 2018
FROM: Linda Ricci
Associate Dir Digital Health, ODE

TO: DEN180042
Irregular Rhythm Notification Feature ([b) (4)

Linda J. Ricci -S
2018.09.08 12:17:26 -04'00'
Linda Ricci

I. INTRODUCTION

The indications for use are:

> The Irregular Rhythm Notification Feature is a software-only mobile medical application that is intended to be used with the Apple Watch. The feature analyzes pulse rate data to identify episodes of irregular heart rhythms suggestive of atrial fibrillation (AFib) and provides a notification to the user. The feature is intended for over-the-counter (OTC) use. It is not intended to provide a notification on every episode of irregular rhythm suggestive of AFib and the absence of a notification is not intended to indicate no disease process is present; rather the feature is intended to opportunistically surface a notification of possible AFib when sufficient data are available for analysis. These data are only captured when the user is still. Along with the user's risk factors, the feature can be used to supplement the decision for Afib screening. The feature is not intended to replace traditional methods of diagnosis or treatment.
>
> The feature has not been tested for and is not intended for use in people under 22 years of age. It is also not intended for use in individuals previously diagnosed with AFib.

Details of the software review are well documented in Nathalie Yarkony's memo. Dr. Yarkony provided a very thorough and scientifically based assessment of the submission.

The purpose of this memo is to document and assess the interactive review elements related to software, address the remaining software deficiencies identified by Dr. Yarkony and provide a final software assessment.

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

(b) (4)

[redacted]

III. Conclusion

As documented above, I believe that the sponsor has addressed all of the remaining software deficiencies and from a software perspective, the file can be granted.