From: OC GCP Questions
To: [redacted]
Subject: Questions regarding 21 CFR part 11 compliance
Date: Thursday, November 17, 2016 10:55:00 AM
Attachments: [redacted]

Good morning –

Please see the answer below from Center for Drugs (CDER) Office of Medical Policy (OMP),

Kind regards,

Doreen M. Kezer, MSN
Senior Health Policy Analyst
Office of Good Clinical Practice
Office of the Commissioner, FDA

Here is our cleared response:

Question 1: [redacted] is planning to utilize a 21 CFR part 11 compliant version of DocuSign for electronic signatures on regulatory documents for clinical trials. We've completed an internal review of compliance with our IT and information security teams and are currently working on the FDA notification letter. I was wondering if other groups have started utilizing e-signatures for regulatory documentation. Have any institutions utilizing e-signatures for regulatory been audited by the FDA? Are there specific pitfalls that we should be aware of before we begin implementation?

Yes, other groups have started using e-signatures for regulatory documentation and have been audited by the FDA. The specific pitfalls that you should be aware of before implementation of electronic signatures on regulatory documents for clinical trials are:

- Not having a secure process to authenticate signers
- Not programming timeouts and log-outs necessitating the re-entry of a password to gain access to the system
- Not linking electronic signatures to the document signed
- Not implementing safeguards to immediately detect and report unauthorized attempts to use signatures
- Not having a process for an emergency to allow a person to "authorize" another person to use his/her signature
- Not having an audit trail to track when the document was signed and who signed it
- Not having the ability to have multiple signers for a document

Question 2: Our institution is utilizing RedCap which is a system that was originally developed by a multi-institutional consortium initiated at Vanderbilt University. Although RedCap is HIPAA compliant, we have questions about utilizing the data entered into RedCap as source documentation There are two scenarios that investigators would like to implement at Cedars-Sinai and I want to know if they would meet 21 CFR part 11.

a. Interviewer-led questionnaires: Study staff interview patients and enter responses directly into the RedCap database system. The system can be programmed to require electronic sign-off by study staff (with a password meeting 21 CFR regulations) and record locking which automatically starts the audit trail per 21 CFR part 11.

   Response: For this scenario above, the information that you've provided is insufficient to determine whether the RedCap database system meets the requirements in 21 CFR part 11. While access controls and audit trails are important components for part 11 compliant systems, there are also other procedures and controls that are necessary to ensure the authenticity, integrity, and the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. For these other procedures and controls, please see 21 CFR 11.10 and 11.30. In addition, electronic signatures must comply with all applicable requirements under 21 CFR part 11 such as the following:

   - Electronic records that are electronically signed must contain information associated with the signing that clearly indicates the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature (see § 11.50).

- The name, date and time, and meaning are subject to the same controls as electronic records and must be included as part of any human readable form of the electronic record (see § 11.50(b)).
- Electronic signatures and handwritten signatures executed to electronic records must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means (§ 11.70).
- The regulations found at 21 CFR part 11 require that an organization verify the identity of an individual before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature or any element of such electronic signature (see 21 CFR 11.100(b)). FDA regulations do not specify any particular method for verifying the identify of an individual and accepts many different methods. For example, verifying someone's identity can be done by using information from some form of official identification, such as a birth certificate, government-issued passport, or a driver's license. In addition, use of security questions, to confirm an individual's identity can also be considered.
- Electronic signatures not based on biometrics must comply with all electronic signature components and controls (see 21 CFR 11.200) and controls for identification codes/passwords (see 21 CFR 11.300).
- Validation is critical to ensure that the electronic system is correctly performing its intended function. Validation may include, but is not limited to, demonstrating correct installation of the electronic signature system and testing of the electronic signature system to ensure that it functions in the manner intended.

b. Patient-facing questionnaires: Patients are sent a link to complete a questionnaire in RedCap. Unfortunately, patients do not have logins for these questionnaires and are also unable to "sign" them per 21 CFR part 11. In order to set up logins and passwords, it would require additional PHI to be collected and maintained in our IT department. For the patient-facing questionnaires, is activating the audit trail upon completion enough for these questionnaires to be considered compliant with 21 CFR part 11 and able to be utilized for Source documentation.

Response: No, this would not be sufficient to meet requirements found in part 11. Also it does not appear to meet the principles of eSource. If a study participant actively participates in the performance measure by entering and submitting data directly to the sponsor's EDC system (e.g., when completing a questionnaire or using an ePRO app), you must have access controls in place to ensure that entries come from the study participant (see 21 CFR 11.10(d)) and the study participant should be identified as the data originator. When data are transmitted to the sponsor's EDC system, the audit trail begins at the time the data enter the sponsor's EDC system. The electronic system used by the study participant should be designed to capture and transmit the following information to the sponsor's EDC system:

- The data originator (i.e., study participant or mobile technology)
- The date and time that data were automatically transferred to the sponsor's database or date and time that data were entered by the study participant

The electronic system should be designed to prevent unauthorized modifications to the data before that data are transmitted to the sponsor's EDC system and only clinical investigators or delegated study personnel who are authorized to make changes should perform modifications or corrections to the data.

Question 3: Is the FDA willing to biometrics based security authentication in lieu of traditional passwords for 21 CFR part 11? For example, could thumbprint authentication be utilized?

FDA accepts electronic signatures based on biometrics. Suitable biometrics must be designed to ensure that they cannot be used by anyone other than their genuine owners (§ 11.200(b)) and they should be uniquely identified with the individual and should not change over time. FDA does not specify any particular biometric method upon which an electronic signature may be based. Electronic signatures based on biometrics are accepted if they meet the requirements found in the part 11 regulations, as stated above (i.e., the signed electronic record must contain pertinent information associated with the signing (see § 11.50), the electronic signatures are subject to the same controls as the electronic records and must be included as part of any human readable form of the electronic record (see § 11.50(b), and the electronic signature must be linked to its respective electronic records (§ 11.70)). In addition, biometrics should be performed based on government and industry standards. For example, the various government agencies and standards development organizations that develop biometric standards include the following:

- National Institute of Standards and Technology
- International Committee for Information Technology Standards
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical

Committee 1/Subcommittee 37

- Organization for the Advancement of Structured Information Standards
- American National Standards Institute

From: [redacted]
Sent: Sunday, November 13, 2016 12:19 PM
To: OC GCP Questions
Subject: Questions regarding 21 CFR part 11 compliance

I am contacting you because [redacted] is working to embrace new technologies and electronic data capture systems to better support research efforts and we want to ensure that we are following FDA and GCP guidelines as we make this transition.

I have several questions that I would like to discuss. Please see below.

1. The [redacted] is planning to utilize a 21 CFR part 11 compliant version of DocuSign for electronic signatures on regulatory documents for clinical trials. We've completed an internal review of compliance with our IT and information security teams and are currently working on the FDA notification letter. I was wondering if other groups have started utilizing e-signatures for regulatory documentation. Have any institutions utilizing e-signatures for regulatory been audited by the FDA? Are there specific pitfalls that we should be aware of before we begin implementation?

2. Our institution is utilizing RedCap which is a system that was originally developed by a multi-institutional consortium initiated at Vanderbilt University. Although RedCap is HIPAA compliant, we have questions about utilizing the data entered into RedCap as source documentation There are two scenarios that investigators would like to implement at Cedars-Sinai and I want to know if they would meet 21 CFR part 11.

   a. Interviewer-led questionnaires: Study staff interview patients and enter responses directly into the RedCap database system. The system can be programmed to require electronic sign-off by study staff (with a password meeting 21 CFR regulations) and record locking which automatically starts the audit trail per 21 CFR part 11.

   b. Patient-facing questionnaires: Patients are sent a link to complete a questionnaire in RedCap. Unfortunately, patients do not have logins for these questionnaires and are also unable to "sign" them per 21 CFR part 11. In order to set up logins and passwords, it would require additional PHI to be collected and maintained in our IT department. For the patient-facing questionnaires, is activating the audit trail upon completion enough for these questionnaires to be considered compliant with 21 CFR part 11 and able to be utilized for Source documentation.

3. Is the FDA willing to biometrics based security authentication in lieu of traditional passwords for 21 CFR part 11? For example, could thumbprint authentication be utilized?

[redacted]