April 2014

FDASIA Health IT Report

Proposed Strategy and Recommendations for a Risk-Based Framework

The Office of the National Coordinator for Health Information Technology

Table of Contents

1. EXECUTIVE SUMMARY

A nationwide health information technology (health IT) infrastructure can offer tremendous benefits to the American public, including the prevention of medical errors, improved efficiency and health care quality, reduced costs, and increased consumer engagement. However, if health IT is not designed, developed, implemented, maintained, or used properly, it can pose risks to patients.

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA), Public Law 112-144, requires that the Food and Drug Administration (FDA), in consultation with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC) (collectively referred to for purposes of this report as "the Agencies"[1]), develop and post on their respective web sites "a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication." This report fulfills the Section 618 requirement.

Health IT incorporates a wide range of products, technologies, and services designed for use by health care entities, health care providers, and consumers, to electronically maintain, access, and exchange health information. Throughout the report, the Agencies' proposed strategy and recommendations are based on the premise that risk and corresponding controls should focus on health IT functionality – not the platform(s) on which such functionality resides or the product name/description of which it is a part. Further, our proposed strategy and recommendations seek to advance a framework that is relevant to current functionalities and technologies yet sufficiently flexible to accommodate the future and rapid evolution of health IT.

The proposed strategy and recommendations reflect the Agencies' understanding that risks to patient safety and steps to promote innovation: 1) can occur at all stages of the health IT product lifecycle; and 2) must consider the complex sociotechnical ecosystem in which these products are developed, implemented, and used. We believe a limited, narrowly-tailored approach that primarily relies on ONC-coordinated activities and private sector capabilities is prudent. We also recommend that no new or additional areas of FDA oversight are needed. Rather, we believe a better approach is to foster the development of a culture of safety and quality; leverage standards and best practices; employ industry-led testing and certification; and selectively use tools such as voluntary listing, reporting, and training to enable the development of a healthcare environment that is transparent and promotes learning to foster continual health IT improvement. Overall, we do not believe that regulation should be or needs to be the first approach used to reach this outcome.

The Agencies' proposed strategy identifies three categories of health IT: 1) administrative health IT functions, 2) health management health IT functions, and 3) medical device health IT functions. We believe that administrative health IT functionalities, such as billing and claims processing, practice and inventory management, and scheduling pose limited or no risk to patient safety and, thus, do not require additional oversight. Health management functionalities include, but are not limited to, health information and data exchange, data capture and encounter documentation, electronic access to clinical results, most clinical decision support, medication management, electronic communication and coordination, provider order entry, knowledge management, and patient identification and matching. We believe the potential safety risks posed by health management health IT functionality are generally low compared to the potential benefits and that strategies to assure a favorable benefit-risk profile of

1 ONC is not an Agency, but an Office, within the Department of Health and Human Services.

these functionalities should adopt a holistic view of the health IT sociotechnical system. As such, if a product with health management health IT functionality meets the statutory definition of a medical device,[2] FDA does not intend to focus its oversight on it. Rather, FDA would focus its attention and oversight on medical device health IT functionality, such as computer aided detection software, remote display or notification of real-time alarms from bedside monitors, and robotic surgical planning and control. Such products are already the focus of FDA's oversight because they generally pose greater risks to patient safety than administrative or health management health IT functionality and FDA oversight is better suited to provide assurance of safety and effectiveness for these functionalities.[3]

The Agencies' proposed strategy and recommendations focus primarily on a risk-based framework for health management health IT functionalities. We identify the following four key priority areas and outline potential next steps that could be taken to help more fully realize the benefits of health IT:

I. Promote the Use of Quality Management Principles;
II. Identify, Develop, and Adopt Standards and Best Practices;
III. Leverage Conformity Assessment Tools; and
IV. Create an Environment of Learning and Continual Improvement.

These priority areas share three critical characteristics: 1) their application can be tailored using a risk-based approach; 2) they have relevance at all stages of the health IT product lifecycle and to all health IT stakeholders; and 3) they support both innovation and patient safety. In each of these priority areas, we believe the private sector can play a strong role.

The Agencies have also identified an additional key component of the health management health IT framework: the creation of a Health IT Safety Center. This public-private entity would be created by ONC, in collaboration with FDA, FCC, and the Agency for Healthcare Research and Quality (AHRQ), with involvement of other Federal agencies, and other health IT stakeholders. The Health IT Safety Center would convene stakeholders in order to focus on activities that promote health IT as an integral part of patient safety with the ultimate goal of assisting in the creation of a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing and ongoing efforts.

The Agencies recognize the importance of health IT to our Nation's health as well as the significance stakeholder input will play in the development of a risk-based framework for health IT that promotes innovation, protects patient safety and avoids regulatory duplication. The proposed framework and priority areas contained in this report are not binding, do not create new requirements or expectations for affected parties, and do not create or confer any rights for or on any person. The Agencies seek public comment on whether the focus areas identified in this report are the appropriate ones – and whether the proposed next steps, described below, will lead to an environment where patient safety is protected, innovation is promoted, and regulatory duplication is avoided. We also plan to convene a public meeting on the proposed strategy and recommendations included in this report within 90 days of the report's release. After receiving public input and finalizing our proposed strategy and recommendations, the Agencies intend to actively engage stakeholders in an ongoing collaborative effort to implement the framework.

2 "Device" is defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. § 321(h). That provision defines a device as "…an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory", that is "… intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man…" or "… intended to affect the structure or any function of the body of man or other animals …." "Medical device" as used in this report has the same meaning as "device."

3 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. September 25, 2013. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

2. BACKGROUND

2.1. Introduction

A nationwide health information technology (health IT) infrastructure can offer tremendous benefits to the American public, including the prevention of medical errors, a reduction in unnecessary tests, increased patient engagement, advancement of the delivery of patient-centered medical care, improvements in the efficiency and coordination of care and information exchange among healthcare providers and organizations, facilitating the identification of and rapid response to public health threats and emergencies, and fostering health-related research. These benefits translate into meaningful improvements in health care quality and clinical outcomes. Thus, there is a strong public health case for the continued use and dissemination of health IT. [4,5]

However, when health IT is not designed, implemented or maintained properly, it can pose risks to patients.[6]

Section 618 of the Food and Drug Administration Safety and Innovation (FDASIA), requires that the Food and Drug Administration (FDA), in consultation with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC), develop and post on their respective web sites "a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication." This report fulfills the Section 618 requirement.

2.2. Overview of Agencies (FDA, ONC and FCC)

The Agencies have different, but complementary, authorities and responsibilities related to the promotion and oversight of health IT in the U.S.

2.2.1. FDA

Using the risk-based approach first established by the Medical Device Amendments of 1976,[7] the Food and Drug Administration (FDA) is responsible for assuring the safety and effectiveness of medical devices (see Appendix 9.1 for additional details). The Agency also facilitates medical device innovation and expedites patient access to high quality medical devices by using a variety of approaches including the promotion and adoption of consensus standards, the selected use of premarket review (approximately 50% of devices are not subject to premarket review prior to marketing), tailored use of 3rd party premarket review and inspection programs, and utilization of postmarket surveillance.

The Agency has more than four decades of experience with "stand alone" and embedded medical device software and has been regulating software with medical device functionality on mobile platforms for more than a decade. FDA's guidance on Mobile Medical Applications

4 David W. Bates, Jonathan M. Teich, Joshua Lee, et al.; "Research Paper: The Impact of Computerized Physician Order Entry on Medication Error Prevention," J Am Med Inform Assoc 1999; 6: 313-321.

5 Basit Chaudhry, Jerome Wang, Shinyi Wu, et al., "Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care," Ann Intern Med 2006; 144(10): 742-752.

6 IOM (Institute of Medicine). 2012. Health IT and Patient Safety: Building Safer Systems for Better Care. Washington, DC: The National Academies Press.

7 The Medical Device Amendments of 1976 created three device classes. The three classes are based on the degree of control necessary to assure that various types of devices are safe and effective. Class I devices are generally low risk. Such devices are for the most part exempt from premarket review and are subject – unless exempt –to the requirements for reporting of adverse events, manufacturing and design controls, registration and listing, and other "general" controls. Class II devices generally present moderate or well-understood risks. Such devices are subject to general controls and are usually subject to premarket review. Class II devices are also subject to "special controls" that are closely tailored to the risks of the particular device type. Class III devices generally present high or poorly understood risks. In addition to general controls, Class III devices are subject to premarket approval and certain other regulatory controls.

articulated the Agency's narrowly focused approach to oversight of these products that considers functionality rather than platform.[8] As stated in the guidance, the Agency does not regulate the sale or general consumer use of smartphones or tablets or consider entities that exclusively distribute mobile medical apps (e.g. the owners and operators of the "iTunes App store" or the "Android market") to be medical device manufacturers. Nor does the Agency consider mobile platform manufacturers to be medical device manufacturers just because their mobile platform could be used to run a product regulated by FDA. FDA recognizes the importance of implementing a balanced, transparent approach to medical device oversight and seeks to strike the right balance by focusing its regulatory resources to provide a risk-based approach to the oversight of those products that present a greater risk to patients if they do not work as intended.

2.2.2. ONC

The Office of the National Coordinator for Health Information Technology (ONC) was created within the Department of Health and Human Services (HHS) first by Executive Order 13335 on April 27, 2004,[9] and then through the Health Information Technology for Economic and Clinical Health (HITECH) Act passed as part of the American Recovery and Reinvestment Act (Recovery Act) of 2009.[10] ONC's responsibilities include, but are not limited to, authoring regulations to adopt standards and certification criteria for health IT; administering certification programs for health IT; supporting two Federal Advisory Committees;[11,12] administering programs to promote electronic health information exchange as well as practice transformation through Regional Extension Centers; promoting health IT policy that empowers patients and their caregivers; promoting standards development and innovative initiatives to advance the science behind health IT; and coordinating the health IT policy and programs of HHS with those of other relevant federal agencies (see Appendix 9.2 for additional details). ONC has a proven track record for bringing stakeholders together to solve big challenges and is committed to seeing that health IT is designed safely, used safely, and attributed oversight that is commensurate with its risks.

2.2.3. FCC

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. It was established by the Communications Act of 1934 and operates as an independent U.S. government agency overseen by Congress. The FCC oversees the authorization of equipment using the radio frequency spectrum and is also responsible for governing the interference potential of equipment which emits radio frequency energy. It does this by first establishing technical regulations for transmitters and other equipment to minimize their potential for causing interference to radio services and then administering an equipment authorization program to ensure that equipment reaching the market complies with the technical requirements. The equipment authorization program requires that equipment be tested to ensure that it complies with the technical requirements prior to marketing. FCC is committed to accelerating the adoption of health care technologies to improve health outcomes and lower health care costs. A more detailed list of recent FCC activities is provided in Appendix 9.3. FCC works closely with FDA, ONC, and other public and private stakeholders.

2.3. Health IT Policy Committee FDASIA Workgroup and Public Input

Section 618(b) of FDASIA permits the Secretary of the Department of Health and Human Services (HHS) to convene a working group of external stakeholders and

8 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. September 25, 2013. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

9 Exec. Order No. 13335, 69 Fed. Reg. 84, 24059 (April 30, 2004) ("The National Coordinator shall [coordinate the development and implementation of] interoperable health information technology.").

10 Health Information Technology for Economic and Clinical Health (HITECH) Act. Pub. L. 111-5, 123 Stat. 115, Division A, Title XIII & Division B, Title IV. The HITECH Act directs the National Coordinator to coordinate the development of a nationwide health IT infrastructure that, *inter alia*, "reduces medical errors" and "improves health care quality." 42 U.S.C. § 300jj-11(b).

11 Health IT Policy Committee. Available at: http://www.healthit.gov/FACAS/health-it-policy-committee.

12 Health IT Standards Committee. Available at: http://www.healthit.gov/FACAS/health-it-standards-committee.

experts to provide appropriate input on the strategy and recommendations that are included in this report. The Secretary decided to convene such a multi-stakeholder workgroup (the "FDASIA Workgroup" or "Workgroup")[13] under the ONC Health IT Policy Committee. The ONC Health IT Policy Committee is a federal advisory committee established by the HITECH Act[14] and is subject to the Federal Advisory Committee Act[15]. The ONC Health IT Policy Committee and the FDASIA Workgroup held open meetings, made documents and information discussed available to the public, and solicited public input during each of its meetings and through a public docket[16].

The FDA, ONC and FCC publicly solicited applications for membership on the FDASIA Workgroup and to the extent practicable, established a Workgroup with membership that was geographically diverse and included experts representing patients, consumers, health care providers, startup companies, health plans, venture capitalists, IT and health IT vendors, small businesses, purchasers, and employers.[17] The FDASIA Workgroup consisted of 28 public members and an ex officio representative from each of the three Agencies. The Workgroup was charged with making recommendations to inform the development of this report and a risk-based framework for health IT that promotes innovation, protects patient safety and avoids regulatory duplication.[18] The FDASIA Workgroup was asked to build on prior work such as the Institute of Medicine (IOM) report entitled Health IT and Patient Safety: Building Safer Systems for Better Care;[19] ONC's Health IT Patient Safety Action and Surveillance Plan;[20] FDA's Mobile Medical Applications Guidance[21] and Medical Device Data Systems Rule[22]; FCC's National Broadband Plan[23] and other relevant work.

The FDASIA Workgroup convened its first meeting on April 29, 2013. The Workgroup divided itself into the following 3 subgroups: taxonomy of health IT, health IT risk assessment and innovation, and health IT regulations. The Workgroup and its subgroups held dozens of virtual meetings and an in-person meeting on May 30-31, 2013. The FDASIA Workgroup presented draft recommendations to the ONC Health IT Policy Committee on August 7, 2013, and final recommendations on September 4, 2013. The FDASIA Workgroup recommendations were accepted and adopted as recommendations of the ONC Health IT Policy Committee at its September 4, 2013 meeting.[24]

2.3.1 Summary of FDASIA Workgroup Recommendations

The work product and recommendations of the FDASIA Workgroup were a direct result of its research, experience, deliberations, and consideration of public input received during its meetings and through the public docket. The Workgroup's recommendations and supporting materials included:

1) A taxonomy for considering the parameters of health IT and consideration of what types of health IT might be subject to a regulatory framework;
2) Suggestions to promote innovation in both the short and long-term while maintaining patient safety;
3) A description of current regulatory frameworks, including perceived ambiguities, deficiencies, and duplication; and
4) Options for the development of a risk framework, including means for stratifying health IT by risk, supplemented by specific health IT use cases.

13 FDASIA. Available at: http://www.healthit.gov/FACAS/health-it-policy-committee/hitpc-workgroups/fdasia
14 Health Information Technology for Economic and Clinical Health (HITECH) Act. Public Law 111-5, February 17, 2009. 123 STAT. 227.
15 The Federal Advisory Committee Act (5 U.S.C. App.), other than section 14 of such Act, applies to the Health IT Policy Committee. Ibid.
16 Food and Drug Administration Safety and Innovation Act (FDASIA): Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology. Comments available at: http://www.regulations.gov/#!docketDetail;D=HHS-OS-2013-0003
17 FDASIA. Available at: http://www.healthit.gov/FACAS/health-it-policy-committee/hitpc-workgroups/fdasia
18 Ibid.
19 IOM (Institute of Medicine). 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press.
20 ONC, *Health Information Technology Patient Safety Action & Surveillance Plan*. July 2, 2013. Available at: http://www.healthit.gov/sites/default/files/safety_plan_master.pdf.
21 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. September 25, 2013. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.
22 Food and Drug Administration. Medical Devices: Medical Device Data Systems. Final Rule. 76 FR 8637 (February 15, 2011).
23 Federal Communications Commission. National Broadband Plan. Available at: http://www.broadband.gov/download-plan/.
24 HIT Policy Committee. Available at: http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it (February 20, 2014).

The Workgroup recommendations included guiding principles for establishing a health IT taxonomy, including the principle that a risk-based approach should focus on the functionality of the health IT product and treat functionality the same across platforms (i.e., functionality should not be treated differently simply because it is on a mobile versus a non-mobile platform). The Workgroup developed a matrix that could be used to assess factors to consider when evaluating the potential risk of the use of health IT. It illustrated how this risk matrix and its many dimensions could apply to personal health records (PHRs), electronic health records (EHRs), clinical decision support (CDS), and various mobile applications. Overall, and as a result of piloting this approach, the Workgroup concluded that it was difficult to categorize complex health IT functionality because of numerous context-specific interdependencies. The Workgroup recommended that: 1) the Agencies could assist stakeholders by providing clearer criteria for how determinations to apply regulatory oversight to health IT functionality would be made; and 2) a surveillance mechanism is needed to track adverse events and near misses for certain health IT functionality that is not regulated. The Workgroup identified ways that the three Agencies could improve certain ambiguities in their guidance and regulations as well as collaborate in issuing future guidance and regulations. The Workgroup provided recommendations for a health IT regulatory framework that included developer and product accountability and transparency at the national level to improve the health IT safety. The workgroup also recommended "local" accountability (rather than "national regulation") through a local control system or accreditation to address local configuration, implementation, and training of end users.

In this report, we highlight specific FDASIA Workgroup recommendations that were adopted by the ONC Health IT Policy Committee, where relevant. In doing so, we use the recommendations as both guiding principles and as a foundation to build upon with more specific and tangible actions. The FDASIA Workgroup membership roster and a complete set of the Workgroup recommendations are available at: http://www.healthit.gov/facas/FACAS/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it (February 20, 2014).

2.3.2. Summary of Public Comments in Response to Federal Register Notice

As part of the development of this report, the Agencies sought broad public input on issues related to FDASIA Section 618 through a notice published in the Federal Register[25]. The Agencies also specifically solicited input on topics identified by the FDASIA Workgroup including health IT taxonomy, risk and innovation, and regulation. Specific questions included:

- What types of health IT should be addressed by the report developed by FDA, ONC, and FCC?
- What factors or approaches could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety?
- Are there current areas of regulatory overlap among FDA, ONC, and/or FCC and if so, what are they? If there are areas of regulatory overlap, what, if any, actions should the agencies take to minimize this overlap?
- How can further duplication be avoided?

The Agencies accepted public comment from May 30, 2013 until August 31, 2013, and comments received by June 30, 2013 were also forwarded to the FDASIA Workgroup for consideration.

A total of 39 comments were received from a wide range of stakeholders including the health IT industry, standards developing organizations, insurers, health care providers, patient advocates, consumers, the medical device industry, associations representing hospitals, pharmaceutical research and biotechnology companies, broadband and telecommunications companies, and non-profit policy and medical research organizations. Commenters recognized both the benefits and risks to patients of health IT. Comments received proposed the following key characteristic requirements for the

25 Office of the National Coordinator for Health Information Technology, Department of Health and Human Services. Food and Drug Administration Safety and Innovation Act (FDASIA): Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology. 78 FR 32390 (May 30, 2013).

framework:

Public Comments Received on Taxonomy:

- Health IT should be assigned into one of three categories: administrative software, clinical software, and medical device software.
- The full range of health IT products should be reviewed to carefully judge the risk to patients.

Public Comments Received on Risk and Innovation:

- Risk assessment for health IT should focus on functionality.
- A health IT learning environment should be created through the aggregation and analysis of data to identify and monitor trends, mitigate future risk, and facilitate learning and improvement.
- Health IT should use existing voluntary safety reporting systems, and patient safety adverse events should be reported in a non-punitive environment by leveraging Patient Safety Organizations.
- Health IT should leverage recognized standards for assuring patient safety.

Public Comments Received on Regulation:

- The health IT regulatory framework should be flexible, agile and evolving to encompass future technology solutions and capabilities without being narrowly prescriptive.
- Quality Management Systems should allow manufacturers to apply a single process that satisfies the requirements of all agencies. Existing safety and quality-related processes, systems, and standards should be leveraged for patient safety in health IT.
- Clinical software development should adopt quality management principles and processes, and apply applicable standards.
- Agency roles should be clarified and avoid overlap. The Agencies individual focuses, such as ONC's focus on privacy, security and health IT infrastructure, and FDA's focus on public health and safety, should be delineated and maintained.
- Emphasis should be placed on the importance of interoperability. The inability of systems to easily and reliably share data can pose safety risks. Due to the current lack of clear or complete oversight of health IT interoperability, a national strategy should be developed to create efficient, standardized data exchange that promotes the safe use of the data that has been exchanged; identify funding to support development of standards; and establish interoperability standards that reflect today's need for rapid development and adoption.
- Outreach activities should be conducted to provide opportunities for collaboration and public input. Examples of outreach would include: ongoing development and dissemination of best practices in the safe design, development, deployment and use of EHRs; creation of useful guidance; and proactive education of developers, through user friendly web-based information and face-to-face educational programs.

3. HEALTH IT: LIFECYCLE AND SOCIOTECHNICAL SYSTEM CONSIDERATIONS

An understanding of the health IT product lifecycle is critical to the development of a narrowly-tailored, predictable regulatory framework that fosters the development of novel technologies, permits timely deployment of iterative product improvements, and routinely identifies underperforming products in a timely fashion. Furthermore, it is important to recognize that health IT products and technologies are not used in isolation. Rather, they are part of a larger sociotechnical system that includes people (e.g. patients and healthcare providers), healthcare organizations, health IT developers and vendors, processes (actions and procedures performed during the delivery of health care), and the environment of use.[26]

3.1 Health IT Product Lifecycle

Stages of the health IT lifecycle include: 1) design and development, 2) implementation and customization, and 3) post-deployment (including upgrades, maintenance, and operations, as well as surveillance, reporting, risk mitigation and remediation)[27] (See FIGURE 1). The safety of health IT relies not only on

26 IOM (Institute of Medicine). 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, DC: The National Academies Press.
27 Id.

how it is designed and developed, but also on how it is customized, implemented, integrated and used.

3.2 Sociotechnical system

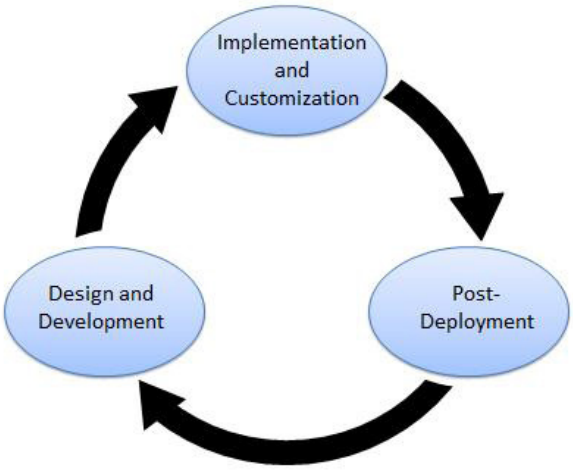
Health IT fits within a complex sociotechnical system. Its successful design, development, implementation, customization and post-deployment use often relies on the integration of many technologies, products, and components by numerous stakeholders. Health IT is designed and developed with varying degrees of quality and rigor by many different developers. It is implemented and customized by organizations with heterogeneous experience and expertise, which poses challenges to the seamless integration of health IT into clinical work flows, and for monitoring, identifying, mitigating, and resolving post-deployment issues in a timely manner. Importantly, safety is a property of the larger system that takes into account how the product is designed, developed, implemented, maintained, and used.

In considering how a sociotechnical system affects the development of a risk-based regulatory framework for health IT, the Agencies recognize that the success – and the safety – of the system as a whole cannot be defined only by the "safety" of individual health IT products themselves. The components of a health IT sociotechnical system include: the technology (e.g. the hardware and software of health IT), the people (e.g. individuals working within the system including healthcare providers and implementers of health IT), the processes (e.g. the workflow of healthcare delivery), the organizations (e.g. how an organization installs and configures health IT) and the external environment (e.g. the environment in which the organizations operate).[28]

The IOM found that several key observations and challenges influence the establishment of a successful health IT system, including: [29]

1) Poorly designed health IT can create new hazards in an already complex system of health care delivery;
2) Individual health IT components may meet their stated performance requirements, yet the system as a whole may yield unsafe outcomes;
3) Problematic events involving complex systems often cannot be ascribed to a single causative factor;
4) Poor human-computer interactions can contribute to serious injury and death;
5) Significant knowledge gaps exist in our

FIGURE 1: Health IT Product Lifecycle



The health IT product lifecycle is depicted. Each stage is characterized by its own distinct considerations for assuring the safe design, development, implementation, customization, integration, and post-deployment use by health care professionals and consumers.

28 Ibid.
29 Ibid.

understanding of the benefits and risks to patients associated with different health IT functionalities.
In summary, an appropriate regulatory framework for health IT should be flexible enough to accommodate innovative, continuously-evolving products undergoing rapid product iterations, upgrades, modifications, and customization, and should account for the complex environment in which the products operate and the multiple stakeholders that play key roles in the successful development, implementation and use of health IT.

4. REPORT SCOPE AND FOCUS OF THE PROPOSED STRATEGY AND RECOMMENDATIONS FOR A RISK-BASED REGULATORY FRAMEWORK

Health IT incorporates a wide range of products, technologies, and services designed for use by health care entities, health care providers, and consumers, to electronically maintain, access, and exchange health information.[30] Throughout the report, the Agencies' proposed strategy and recommendations are based on the premise that risk and corresponding controls should focus on health IT functionality – not on the platform(s) (e.g. mobile, cloud-based, installed) on which such functionality resides or the product name/description of which it is a part.[31] Further, the Agencies' strategy and recommendations seek to advance a framework that is relevant to current functionalities and technologies yet sufficiently flexible to accommodate the future and rapid evolution of health IT.

The Agencies' proposed strategy and recommendations identify three categories of health IT functionality: 1) administrative health IT functions, 2) health management health IT functions, and 3) medical device health IT functions (See FIGURE 2). This paradigm creates health IT functional categories with important distinctions in both risk and proposed corresponding risk controls, although each of the three proposed categories can be designed for use by health care entities, health care providers, patients, and consumers. It is also important to note that the systems that healthcare organizations and consumers are purchasing, implementing and using, often contain functionalities that bridge all three of these categories. For example, electronic health records (EHRs)[32] may have functionality that spans one or more of these categories. Similarly, some functionalities, such as privacy and security, cannot be placed in a single category.[33]

Ultimately, the Agencies recognize that any categorization scheme will be imperfect and may need to adapt over time. Nevertheless, we believe that this proposed functional categorization can both assist the Agencies in avoiding regulatory duplication and prompt meaningful policy discussions with stakeholders to identify and clarify unresolved areas of ambiguity (e.g. instances where categorization into "administrative" vs. "health management" or "health management" vs. "medical device" health IT functionality is unclear).

4.1 Administrative Health IT Functionality

Administrative functionalities, including but not limited to software intended to facilitate admissions, billing and claims processing, practice and inventory management, scheduling, general purpose communications, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, reporting of communicable diseases to public health agencies and reporting on quality measures pose limited or no risk to patient safety. As such, the Agencies recommend

30 Health Information Technology for Economic and Clinical Health (HITECH) Act. Public Law 111-5, February 17, 2009. 123 STAT. 227.

31 Although functionality, and not platform, is the primary focus of this proposed risk-based strategy, certain platform-related issues, such as network connectivity, service availability, and security have important implications for the safe use of health IT.

32 For the purposes of this report an EHR is defined as a real-time patient-centered record that allows access to evidence-based tools that can aid providers in decision-making. The EHR can automate and streamline clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting. See: What is an Electronic Health Record (EHR)? at: http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr.

33 The HHS Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. See Health information Privacy at: http://www.hhs.gov/ocr/privacy/index.html

that no additional oversight of these types of products is necessary to protect patient safety and promote innovation.[34]

4.2 Health Management Health IT Functionality

Health management health IT functionalities (sometimes referred to as "clinical software") include, but are not limited to:

- Health information and data management;
- Data capture and encounter documentation;
- Electronic access to clinical results;
- Most clinical decision support; [35]
- Medication management (electronic medication administration records);
- Electronic communication and coordination (e.g. provider to patient, patient to provider, provider to provider, etc.);
- Provider order entry;
- Knowledge (clinical evidence) management;
- Patient identification and matching.

The Agencies believe the potential safety risks posed by health management health IT functionality are generally low compared to the potential benefits and must be addressed by looking at the entire health IT ecosystem rather than single, targeted solutions. If such health management health IT functionality meets the statutory definition of a medical device, FDA does not intend to focus its regulatory oversight on such functionality because the Agencies' proposed strategy and recommendations for a risk-based framework for health management health IT, outlined in Section 5, can help to assure a favorable benefit-risk profile of these functionalities. Section 5 articulates specific proposed priority areas and potential next steps that could help more fully realize the benefits of health IT.

4.3 Medical Device Health IT Functionality

Health IT with medical device functionality[36] is currently the focus of FDA's oversight. Examples include computer aided detection/diagnostic software, radiation treatment planning, and robotic surgical planning and control software. ONC and FCC may have complementary activities in certain areas (e.g. interoperable data exchange between a medical device and EHR, use of wireless spectrum for wireless medical devices, etc.). The strategy and recommendations for a risk-based health IT framework do not propose the need for new FDA authorities or additional areas of oversight. The FDASIA Health IT Working Group did recommend that the FDA provide greater clarity related to several aspects of medical device regulation involving health IT, including:

1) The distinction between wellness and disease-related claims;
2) Medical device accessories;
3) Medical device clinical decision support software;
4) Medical device software modules;[37] and
5) Mobile medical apps.[38]

These items are discussed in more detail in Section 6.

34 Some existing federal laws and regulations, such as those addressing the confidentiality, privacy and security of electronic patient health information, or those that apply to wireless communications (FCC), are applicable to all 3 categories of health IT (including administrative health IT).

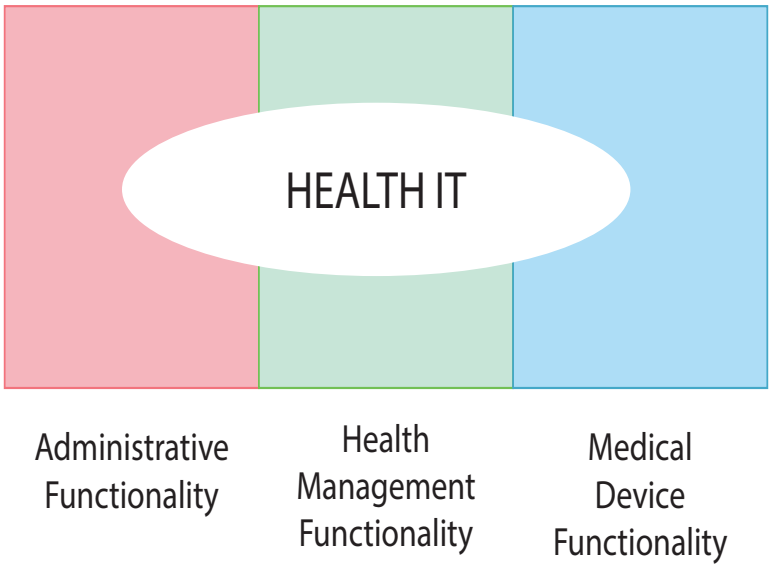
35 Clinical decision support (CDS) provides health care providers and patients with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. Because its risks are generally low compared to the potential benefits, FDA does not intend to focus its oversight on most clinical decision support. FDA, instead, intends to focus its oversight on a limited set of software functionalities that provide clinical decision support and pose higher risks to patients, such as computer aided detection/diagnostic software and radiation therapy treatment planning software. See Section 6 for additional details.

36 Section 201(h) of the FD&C Act defines device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is-- … intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes."

37 Report of the Section 618 Regulations Subgroup – Summary. Available at: http://www.healthit.gov/FACAS/sites/faca/files/FDASIARegulationSummary901413.pdf

38 The FDASIA Workgroup final recommendations accepted and adopted by the ONC Health IT Policy Committee on September 4, 2013, stated that "FDA should expedite guidance on Health IT software, mobile medical apps and related matters". On September 25, 2013, FDA issued final guidance entitled, Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff", available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

FIGURE 2 - Categories of Health IT Functionality



Health IT functionality can be broadly grouped into three categories: 1) administrative health IT functionality, 2) health management health IT functionality, and 3) medical device health IT functionality. Each of the three proposed categories can be designed for use by health care entities, health care providers, patients, and consumers. **Administrative functionalities**, including but not limited to admissions, billing and claims processing, practice and inventory management, scheduling, general purpose communications, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, reporting of communicable diseases to public health agencies and reporting on quality measures pose limited or no risk to patient safety. The Agencies believe no additional oversight of these types of products is necessary. **Health management functionalities** include but are not limited to health information and data exchange, data capture and encounter documentation, electronic access to clinical results, some clinical decision support, medication management, electronic communication and coordination, provider order entry, knowledge management, and patient identification and matching. Health management health IT functionalities are the primary focus of the framework described in this report. If a product with health management health IT functionality meets the statutory definition of a medical device, FDA does not intend to focus its oversight on it - - because the Agencies' proposed strategy and recommendations for a risk-based framework for health management health IT can help to assure a favorable benefit-risk profile of these functionalities. FDA would focus its oversight on **medical device functionality** because, in general, these functions, such as computer aided detection software and remote display or notification of real-time alarms from bedside monitors, present greater risks to patient safety than health IT with administrative or health management functionality.

5. PROPOSED STRATEGY AND RECOMMENDATIONS FOR A HEALTH MANAGEMENT HEALTH IT FRAMEWORK

Health IT has the potential to reduce medical errors, increase the efficiency of healthcare delivery, reduce costs, and improve the quality of healthcare for Americans. However, shortcomings in health IT design, development, implementation, customization, integration and use may result in adverse health consequences. We propose that a framework intended to promote innovation and protect patient safety should adhere to the following principles:

1) Employ a risk-based approach to appropriately mitigate patient safety risks while avoiding unnecessary regulatory oversight;
2) Leverage private sector knowledge, experience, and expertise;
3) Facilitate, rather than impede, innovation;
4) Promote transparency of product performance and safety; and
5) Create/support an environment of learning and continual improvement.

The proposed framework is based on the health IT product lifecycle and the complex sociotechnical system in which these products are developed, implemented, and used, and the extent of risk posed by health IT products. We recommend a limited, narrowly-tailored approach that primarily relies on ONC-coordinated activities and private sector capabilities. For example, we do not recommend the need for any new or additional areas of FDA oversight. Rather, we believe a better approach is to foster the development of a culture of safety and quality, leverage standards and best practices, employ industry-led testing and certification, and selectively use tools such as voluntary listing, reporting, and training to enable the development of a transparent learning healthcare environment that fosters continual health IT improvement. We do not believe that regulation should be, or needs to be, the first approach used to reach this outcome.

This section identifies the four key proposed priority areas for a risk-based framework for health management health IT functionality and outlines potential next steps for each (FIGURE 3):

I. Promote the Use of Quality Management Principles
II. Identify, Develop, and Adopt Standards and Best Practices
III. Leverage Conformity Assessment Tools
IV. Create an Environment of Learning and Continual Improvement

These priority areas share three critical characteristics: 1) their application can be tailored using a risk-based approach; 2) they have relevance at all stages of the health IT product lifecycle and to all health IT stakeholders; and 3) they support both innovation and patient safety.

In addition to the four key priority areas listed in FIGURE 3, the Agencies have identified an additional key component to the health management health IT framework - the creation of a Health IT Safety Center. This public-private entity would be created by ONC, in collaboration with FDA, FCC, and AHRQ, and with involvement of other Federal agencies and health IT stakeholders. The Health IT Safety Center would serve as a trusted convener of health IT stakeholders in order to focus on activities that promote health IT as an integral part of patient safety with the ultimate goal of assisting in the creation of a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing and ongoing efforts. The Health IT Safety Center could enable a deeper understanding of how these four priorities can and should be integrated into the programs and activities of stakeholders in health IT safety. To be successful, the Health IT Safety Center will require a strong governance mechanism and involvement by participants in programs and activities that:

- Establish a broad and engaged stakeholder membership and leadership base;
- Focus on high-value issues affecting the promotion of innovation and the protection of patient safety related to health IT;
- Build upon and improve the evidence-based foundation for health IT safety by analyzing the best available data and evidence and by identifying interventions and opportunities for

improvement based on the data and evidence;
- Create or inform health IT safety priority goals and measures that align with broader patient safety goals and initiatives;
- Provide education on health IT safety, including on best practices regarding risks, mitigation strategies, usability, workflow, etc. to improve the commitment and capabilities of participant organizations to improve their health IT safety efforts and evaluate the effects of that education.

The Agencies believe this type of collaborative public private effort is critical to the successful implementation of the strategy and recommendations contained in this report.

The Agencies seek input on whether the focus areas identified in this report are the appropriate ones – and whether the proposed next steps, described below, will lead to an environment where patient safety is protected, innovation is promoted, and regulatory duplication is avoided. The Agencies also seek comment on what steps should be taken to encourage and foster private sector participation in the identified priority areas and in the Health IT Safety Center. The Agencies believe such participation could help otherwise avoid the need for a more active regulatory approach while assuring that health IT risks are minimized and patient safety protected.

Summary and Conclusion:

The Agencies' strategy and recommendations for a risk-based framework for health management health IT include four key priority areas: promote the use of quality management principles; identify, develop, and adopt standards and best practices; leverage conformity assessment tools; and create an environment of learning and continual improvement. The Agencies also recommend the creation of a Health IT Safety Center as a public-private entity with broad stakeholder engagement, that includes a governance structure for the creation of a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing and ongoing efforts.

5.1 Promote the Use of Quality Management Principles

Quality management principles and processes, as part of a quality system, have been adopted and implemented by more than 1 million companies and organizations worldwide to improve quality, efficiency, safety and reliability.[39] The selective adoption and application of existing quality management principles and processes to health IT has been advocated by the IOM[40], the FDASIA Workgroup, and numerous health IT stakeholders including developers, implementers and users. Some, but not all, health IT developers and healthcare facilities already adopt quality management principles.

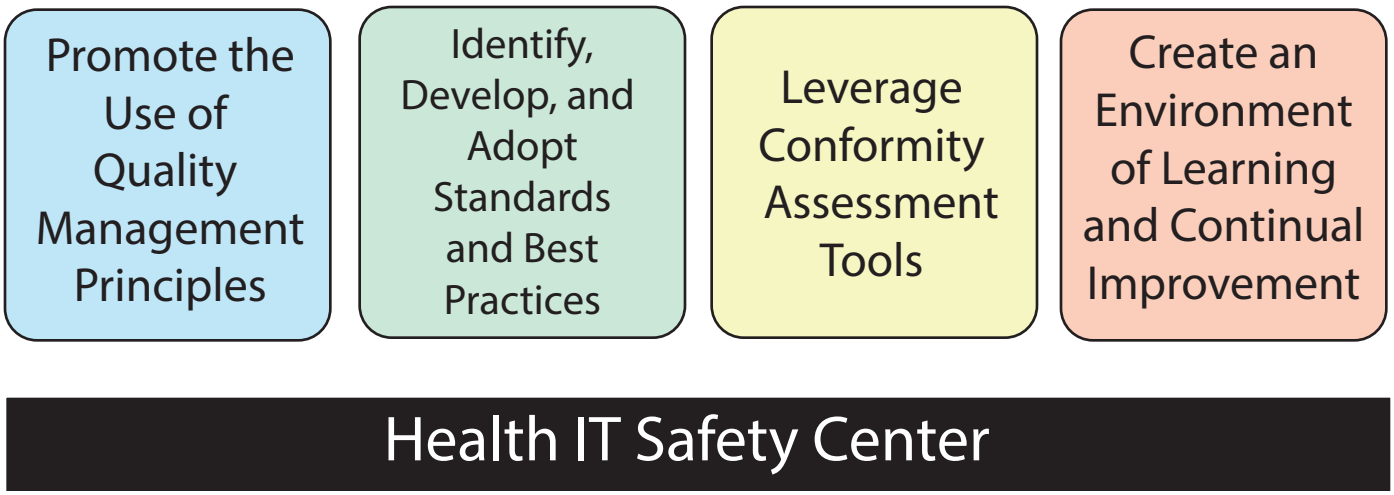
A number of different approaches to quality management exist; however, they share certain common, underlying principles. Quality management principles help to identify, prevent, track, and monitor safety hazards and to reduce risks. They can be applied throughout the product lifecycle to design and development activities, to implementation, customization, integration, upgrades, maintenance, and operations, as well as to surveillance, reporting, risk mitigation and remediation. Importantly, quality management principles are flexible, scalable and adaptable so organizations (e.g. health IT developers, healthcare facilities, etc.) can tailor the application of these standardized processes to their individual circumstances and needs. Ultimately, quality management principles and processes provide a quality framework for companies and organizations to ensure that their products and services consistently meet their customers' needs and requirements, that risk management principles are applied to identify, evaluate, mitigate and remediate hazards, and that overall quality is continually improved.

The judicious application of quality management principles and processes by health IT stakeholders can promote the safe design, development, implementation, customization, integration, and use of health IT while fostering an environment that promotes innovation and continual improvement. However, because health IT represents a broad spectrum of products and services, health IT developers and organizations must

39 See International Organization for Standardization (ISO), *ISO 9000 – Quality Management* at: http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm.

40 IOM (Institute of Medicine). 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press

FIGURE 3: Overview of Proposed Health IT Priority Areas



The proposed risk-based framework for health IT identifies four key proposed priority areas and outlines potential next steps that could be taken to help more fully realize the benefits of health management health IT functionality. **Promoting the use of quality management principles**, including a quality systems approach, by health IT stakeholders is necessary for the safe design, development, implementation, customization, and use of health IT. The **identification, development, and adoption of applicable health IT standards and best practices** can help to deliver consistently high quality health IT products and services to consumers. **Conformity assessment tools** (e.g. product testing, certification, accreditation) can provide assurance that health IT products, services, systems, and organizations meet specified standards or fulfill specified requirements. These tools should be used and applied in a risk-based manner to distinguish high quality products and organizations from those that fail to meet basic performance standards or requirements. The **creation of an environment of learning and continual improvement**, including transparent reporting, aggregation, and analysis of safety issues is central to a health IT framework that promotes innovation and protects patient safety. The Agencies recommend the creation of a Health IT Safety Center that includes broad representation from public and private sector stakeholders to establish a governance structure for the creation of a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing and ongoing efforts.

have flexibility to determine the necessity of individual quality elements and to tailor the development and implementation of quality management processes appropriate for their products and services.

As part of the 2014 Edition Standards and Certification Criteria final rule[41], ONC adopted two safety-related certification criteria for EHRs: one that focuses on the application of user-centered design to medication-related certification criteria and another that focuses on the quality management system (QMS) used during the EHR technology design. In general, the Agencies believe that additional value to health IT purchasers and users could be realized if greater transparency existed around the quality management principles that were applied in the design and development, customization and implementation, and post-deployment use of health IT.

Summary and Conclusion:

The application of quality management principles, including a quality systems approach by health IT stakeholders, is necessary for the safe design, development, implementation, customization, and use of health IT. The Agencies will work with health IT stakeholders to identify the essential elements of a health IT quality framework, leveraging existing quality management principles and identifying areas where quality management principles can or should be applied. The Agencies view this strategy, rather than a formal regulatory approach, as the appropriate method for advancing a health IT quality framework.

The Agencies seek input on the following questions related to promoting the use of quality management principles in health IT:

- *What essential quality management principles should apply to health IT? How should they apply to different stakeholders and at different stages of the health IT product lifecycle?*

- *How do we assure stakeholder accountability for adoption of quality management principles? Is there a role for a non-governmental, independent program to assess stakeholder adherence to quality management principles? Is there a role for government?*

5.2 Identify, Develop and Adopt Standards and Best Practices

The identification, development, and adoption of standards and best practices are a key aspect of a health IT framework that promotes innovation and protects patient safety. Consensus standards, developed through a collaborative, evidence-based, fair, open, and impartial process,[42] provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that products, processes and services are fit for their purpose.[43] Best practices are processes or methods that have been demonstrated to deliver consistently superior results. Like standards, best practices can be used to promote and maintain consistency and quality. Importantly, both standards and best practices allow health IT developers to vary their product design, function, features and development approach, and organizations to tailor their methods and processes to their needs. Standards and best practices can set the minimum expectations necessary to achieve an acceptable level of performance and can serve as a guide for achieving performance excellence.

Many existing domestic and international consensus standards address key aspects of product quality, performance and safety, are relevant to health IT, and have been developed with the participation of FDA, ONC, FCC, AHRQ, other government agencies, and key health IT stakeholders. A number of additional existing standards may be applicable to health IT including but not limited to those pertaining to quality management systems, risk management, interoperability, and software development, validation and lifecycle management.

ONC has responsibility for advancing the development, adoption, and implementation of health IT standards

41 Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services. Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology. 77 FR 54163 (September 4, 2012).

42 Consensus is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties. See Office of Management and Budget (OMB,) CIRCULAR NO. A-119 Revised at http://www.whitehouse.gov/omb/circulars_a119.

43 See International Organization for Standardization (ISO), *Standards* at: http://www.iso.org/iso/home/standards.htm.

nationally through public and private collaboration. The HITECH Act established the Health IT Standards Committee,[44,45] which serves as a forum for the participation of a broad range of stakeholders to provide input on the development, harmonization, and recognition of standards, implementation specifications, and certification criteria necessary for the development and adoption of a nationwide health IT infrastructure that allows for the electronic use and exchange of health information.

5.2.1 Interoperability

Interoperability[46] supports improvements in safety, encourages innovation and facilitates new models of health care delivery by making the right data available to the right people at the right time across products and organizations in a way that can be relied upon and used by recipients. Interoperability permits electronic communication between software applications and across medical devices and electronic health records thereby supporting innovation that can only occur when the data is not "siloed" in one product, technology or system. In addition, it promotes system integration even when products from different vendors are used, and can improve data portability and patient safety. Errors in communication due to inadequate interoperability, such as the transmission of test results inaccurately or for the wrong patient, do occur and can lead to patient harm. Improved interoperability among health management health IT systems, medical devices and administrative systems could catalyze innovation in the health IT marketplace, better support emerging care models, and create greater marketplace competition and responsiveness to end-user needs.

The Agencies have actively fostered the secure and seamless exchange of health information, but challenges remain. This risk-based health IT framework should promote interoperability and electronic information sharing between health IT products and across organizational boundaries. The FDASIA Workgroup recommended that interoperability of health IT could be addressed, in part, through adoption of standards. Standards-based interoperability could facilitate new and innovative health IT products and solutions tailored to address users' needs.

Fostering the development of interoperable products and systems, in part, requires the creation, validation, and recognition of common standards across product categories. ONC has broad responsibility for adopting standards, implementation specifications, and certification criteria for health IT in conjunction with its voluntary certification program, as well as leading policy efforts to effectively encourage and coordinate nationwide health information exchange activities. ONC adopts standards for health IT through regulations and leverages public-private collaboration to identify and specify standards and implementation specifications that could be used through the Standards & Interoperability Framework activity.[47] In 2012, FDA and the Association for the Advancement of Medical Instrumentation (AAMI) organized a summit that brought together hundreds of experts from many disciplines to further the goal of improving patient care and fostering innovation through interoperability. FDA has since recognized a set of voluntary standards pertaining to interoperability and cybersecurity that will help medical device manufacturers create secure devices that work well together and with other health IT products and systems.[48] In February 2014, ONC co-hosted Health Care Innovation DC: Igniting an Interoperable Healthcare System, a conference to provide a venue for stakeholders to collaborate and partner on solutions to achieve interoperability in ways that improve patient care.[49]

The Agencies recommend that entities be identified to develop tests to validate interoperability, test product conformance with standards, and transparently share results of product performance to promote broader adoption of interoperable solutions. Conformance with recognized consensus standards can be used to

44 Health Information Technology for Economic and Clinical Health (HITECH) Act. Public Law 111-5, February 17, 2009. 123 STAT. 227.

45 Health IT Standards Committee. Available at: http://www.healthit.gov/FACAS/health-it-standards-committee.

46 For the purposes of this report, interoperability means "the ability of two or more systems or components to exchange information and to use the information that has been exchanged." See Institute of Electrical and Electronics Engineering (IEEE) Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries (New York, NY: 1990).

47 S&I Framework. Available at: http://www.siframework.org.

48 Under section 514(c) of the FD&C Act, FDA must recognize all or part of an appropriate standard established by a nationally or internationally recognized standard development organization for which a person may submit a declaration of conformity in order to meet a premarket submission requirement or other requirement under the FD&C Act to which such standard is applicable. FDA maintains a list of all currently recognized standards at http://www.fda.gov/cdrh/stdsprog.html.

49 HCI/DC 2014. Available at: http://hcidc.org/

meet certain regulatory requirements.[50] The concept of conformity assessments is discussed in more detail in Section 5.3.

5.2.2 Best Practices for Local Implementation, Customization and Maintenance of Health IT

An important patient safety gap in the current health IT sociotechnical system identified by the IOM, the FDASIA Workgroup, and other health IT stakeholders concerns the local implementation, customization, and maintenance of health IT. This gap may be addressed, in part, by the development and widespread adoption of best practices. Successful implementation of health IT is critical to optimizing its benefits and mitigating patient safety risks. Evidence has shown, however, that implemented and applied inappropriately, health IT can add complexity and result in adverse consequences, such as medication dosing errors, or delays in diagnosis and treatment.

Local implementation and customization of health IT includes its integration into an organization's IT environment, and clinical and administrative workflow. Implementation includes assessing product usability, addressing workflow disruptions, minimizing system downtime, and planning maintenance to keep the system operational and support ongoing use. Clinical implementation incorporates testing, training, deployment and post-deployment stabilization.

In many health IT environments, the introduction of new technologies and products or other system adaptations and modifications are frequent. As a result, system level failures are a risk that can be minimized by having well-established best practices for health IT implementation and routines for responding to system downtime. For example, best practices may address:

- Contingency plans to return the system to normal operations as soon as possible;
- Preparation for interruption of information continuity during unforeseen downtime;
- Routines for the introduction and integration of health IT products into clinical workflows;
- Installation, including testing during implementation;
- Customization, including accountability for product performance when the product is modified and no longer resembles shipped product;
- Information sharing about obstacles encountered during implementation;
- Health IT product assessment after clinical implementation;
- Education, training, knowledge and skill required, including basic levels of competence and
- Health care facility, user, and vendor responsibilities.

In January 2013, ONC released the Safety Assurance Factors for EHR Resilience (SAFER) Guides as a way to assist and encourage health care organizations and providers to identify recommended practices and optimize the safe use of EHRs.[51] The SAFER Guides address many key health IT best practice areas and can serve as useful starting point when attempting to assess potential health IT safety risks.

The development and widespread adoption of best practices for the local implementation, customization and maintenance of health IT could address an important need and should be complemented by a framework that provides independent assessments of organizational conformity to established best practices, with transparency and accountability.

Summary and Conclusions

The identification, development, and adoption of applicable health IT standards and best practices can help to deliver consistently high quality health IT products and services to consumers. The Agencies have identified the following specific focus areas for standards and best practices implementation:

- **Health IT design and development, including usability;**
- **Local implementation, customization and maintenance of health IT;**
- **Interoperability;**

50 For example, where appropriate, FDA typically accepts a declaration of conformity to recognized consensus standards in lieu of actual test data (section 514(c) of the FD&C Act).

51 Safety Assurance Factors for EHR Resilience. Accessed at: http://www.healthit.gov/policy-researchers-implementers/safer.

- **Quality management, including quality systems; and**
- **Risk management.**

The Agencies seek input on the following questions related to identification, development, and adoption of standards and best practices in health IT:

- *Are the identified priority areas for standards and best practices the proper areas of focus? If not, what areas should be prioritized?*
- *How can the private sector help facilitate the development and adoption of applicable health IT standards and best practices? Is there a role for a non-governmental, independent program to assess product and stakeholder adherence to standards and best practices? Is there a role for government?*

5.3 Leverage Conformity Assessment Tools

The adoption of quality management principles and the utilization of standards and best practices can contribute to the design, development, and deployment of high quality health IT products. Product testing, quality assessments, accreditation, certification, and evaluation of adherence to standards, guidelines, or best practices are tools that can enhance transparency, patient safety, and consumer confidence by verifying that a particular product, developer, vendor, or organization meets a specified level of quality, safety, or performance.

These tools, broadly referred to as "conformity assessment tools" in this report, can provide assurance that certain products, services, systems, or organizations fulfill specified requirements. [52,53] Conformity assessment may include certification, testing, inspection, or a declaration of conformity. It may include a self-assessment, or accreditation performed by a third party. It may apply to an entire product, developer or organization or only to a specific performance characteristic, process, or system. In short, conformity assessments are flexible and can be tailored, as appropriate, as part of a risk-based approach.

Conformity assessments can be performed by either the private sector or government. Private sector assessments may have some advantages such as increased efficiency, the promotion of consumer transparency and economic competition, and reduced government costs. In some cases, however, government assessments may be more appropriate, such as when conformity assessments are critical to assuring the safety and health of consumers. When used in appropriate circumstances, conformity assessments can promote competition, innovation and safety, and avoid the creation of unnecessary regulatory barriers. The decision about the types of conformity assessments that bring value to the health IT community and the manner in which they are performed should be developed with broad involvement of health IT stakeholders.

The examples in the subsections below highlight some of the actual and potential uses of conformity assessment tools in health IT. These examples are intended to be illustrative, not an exhaustive list of all possibilities. Importantly, the Agencies do not propose that new or additional mandatory conformity assessments be required prior to the production, marketing, or use of a specific health IT product or service. Instead, we recommend that these tools should be used and applied in a risk-based manner to distinguish high quality products and organizations from those that fail to meet basic performance standards or requirements. The Agencies seek input on the value and role of voluntary conformity assessment tools for various health IT stakeholders during the different stages of the health IT product lifecycle, and whether various types of conformance testing can support innovation, such as by providing assurances during development phases to reduce risk.

5.3.1 Product Testing

Testing of health IT during various stages of its design and development, implementation and customization, and post-deployment can help determine whether the characteristics or performance of a given product or service, including user requirements and needs, have been met. Testing in actual or simulated environments (e.g. during clinical use) can be of value, and some,

52 National Institute of Standards and Technology (NIST). 15 CFR Part 287. *Guidance on Federal Conformity Assessment Activities.* FR Volume 65, No. 155, pages 48894-48902, August 10, 2000. Available at: http://gsi.nist.gov/global/docs/FR_FedGuidanceCA.pdf.

53 See American National Standards Institute (ANSI), *United States Conformity Assessment Principles*, available at: www.ansi.org/ncap.

including the IOM, have advocated that standardized testing procedures should be developed and used by manufacturers and health care organizations to assess the safe design, development, implementation, and deployment of health IT products.[54] In addition, the selective use of test beds[55] can facilitate the rigorous, reproducible, and transparent testing of health IT products or features. Development of post-implementation tests could help users monitor whether their systems meet certain safety benchmarks.

For example, the National Institute of Standards and Technology (NIST), with support from ONC, has developed tools for usability testing of certified EHR technology. In addition, the Strategic Health IT Advanced Research Projects–C (SHARP-C) Program is developing usability testing tools using NIST protocols. NIST and ONC plan to continue to build upon this work, and ONC will use it to strengthen safety-enhanced certification criteria. Non-governmental, independent programs could be developed in key areas to address current gaps.

5.3.2 Certification

Certification is a procedure used to provide written assurance that a product, process, service, or person's qualifications conforms to specified requirements.[56] Certification can be administered by the government or the private sector.

Section 3001(c)(5) of the Public Health Service Act (PHSA) provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the "National Coordinator, in consultation with the Director of the National Institute of Standards and Technology, shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle" (i.e., certification criteria adopted by the Secretary under section 3004 of the PHSA). ONC relied upon this authority to establish the ONC HIT Certification Program. Currently, EHR technology is certified under this program for either the ambulatory or inpatient setting. The ONC Certified Health IT Product List is available at http://oncchpl.force.com/ehrcert. For the consumer, ONC certification provides purchasing clarity and assurance that the certified EHR product meets certain criteria and/or functions in a certain way. While ONC has focused on EHR technology certification, it also has authority to certify other types of health IT.[57]

5.3.3 Accreditation

Accreditation is a procedure used to indicate that a third party or an individual is competent to carry out specific tasks, such as testing, inspection, or certification. For example, a private sector, independent organization could serve as an accrediting body to independently assess an organization for adherence to recognized standards, guidelines, and/or best practices. Accreditation has been applied to health care organizations and providers, and could be used voluntarily at various additional points in the health IT product lifecycle (e.g. assessing vendor compliance with quality principles or health care organization adherence to health IT implementation best practices). Accreditation is typically voluntary, although other entities such as purchasers or payers, may "require" its use.

Voluntary conformity assessment tools, such as certification, product testing, and accreditation could be implemented by the private sector and applied in a risk-based manner to selected health IT.

Summary and Conclusions

Conformity assessment tools, such as product testing, certification and accreditation can provide assurance that certain products, services, systems, or organizations meet specified standards or fulfill certain requirements. The Agencies recommend that these tools should be used and applied in a risk-based manner to distinguish high quality products, developers, vendors and organizations from those that fail to meet a specified level of quality, safety,

54 IOM (Institute of Medicine). 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press.
55 For the purposes of this report, a test bed is a platform or environment that allows for reproducible, rigorous, and transparent product or system evaluation.
56 National Institute of Standards and Technology. 15 CFR Part 287. Guidance on Federal Conformity Assessment Activities. 65 FR 48894-48902 (August 10, 2000). Available at: http://gsi.nist.gov/global/docs/FR_FedGuidanceCA.pdf.
57 Health Information Technology for Economic and Clinical Health (HITECH) Act. Public Law 111-5, February 17, 2009. 123 STAT 232.

or performance. We also recommend that non-governmental, independent programs to perform conformity assessments should be developed to fill current gaps.

The Agencies view this strategy rather than a formal regulatory approach as the appropriate method for advancing conformity assesments.

The Agencies seek input on the following questions related to clarifying the value and role of conformity assessment tools in health IT:

- *What conformity assessment tools, if any, should be incorporated into a risk-based health IT framework? How should they apply to different stakeholders and at different stages of the health IT product lifecycle? How can adoption of and adherence to conformity assessment programs be promoted?*
- *Should interoperability be tested? How should tests to validate interoperability be conducted? Should interoperability standard(s) be adopted and used for conformity assessments (i.e. develop a functional standard that specifies interoperability characteristics that could be used for conformity assessment)?*
- *How should the intended user (e.g. health care provider, consumer, etc.) affect the type of conformity assessment performed?*
- *How should conformance assessment results be communicated to stakeholders?*
- *Is there a role for a non-governmental, independent health IT conformity assessment program? Is there a role for government? Should the ONC Health IT Certification Program be leveraged to protect patient safety through the use of conformity assessment tools?*

5.4 Create an Environment of Learning and Continual Improvement

The creation of an environment of learning and continual improvement is central to a health IT framework that protects patient safety and promotes innovation. Such a system should:

1) Identify, report and respond to health IT-related adverse events and near misses;
2) Aggregate and analyze events and near misses to identify patterns and trends;
3) Share information about methodology, practices, policies, and findings in a transparent manner;
4) Support the development and adoption of interventions and mitigations, where appropriate; and
5) Promote system-wide education and learning for stakeholders resulting in a system that is continually undergoing improvement.

The establishment of an environment of learning and continual improvement with the goal of improving quality and safety of patient care is neither novel nor controversial. The Patient Safety and Quality Improvement Act of 2005 ("Patient Safety Act")[58] was enacted to improve patient safety by encouraging voluntary and confidential reporting of adverse patient safety events to Patient Safety Organizations (PSOs) by clinicians and healthcare organizations without fear of liability.[59]

According to the IOM, several important challenges and contributing factors, however, have impeded the development of a robust health IT learning environment including:[60]

- Persistent underreporting of patient safety events and near misses, even when there are well-established programs in place encouraging health professionals to report;
- A tendency to focus on identifying a single root cause of an adverse event rather than addressing the systems-based nature of many health IT problems;
- Examination of isolated, individual system components rather than evaluating interaction of components in actual practice;
- Failure to recognize adverse events as health IT-related at the time of their occurrence;

58 Public Law 109-41. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-109publ41/pdf/PLAW-109publ41.pdf.
59 42 CFR Part 3. Patient Safety and Quality Improvement. Final Rule. Available at: http://www.pso.ahrq.gov/regulations/fnlrule01.htm.
60 IOM (Institute of Medicine). 2012. *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, DC: The National Academies Press.

- Adoption of a philosophy of "shared responsibility" without well-defined individual stakeholder accountability;
- Focus on the role of technology when safety is compromised without addressing the human-interaction component; and
- Restrictions on the transparent release of safety information through contractual limitations and fear of liability.

The IOM Committee on Patient Safety and Health Information Technology and the FDASIA Workgroup recommended the development of:

- A mechanism for identifying selected health IT products in the marketplace (e.g. listing);
- Standardized formats for reporting health IT patient safety events and near misses;
- Mechanisms to ensure transparency of results;
- Approaches to allow aggregation of safety issues at the national level, with federal support;
- Steps to discourage vendors from engaging in practices that limit the free flow of safety information; and
- Creation of a safety governance structure that includes federal and private sector stakeholders.

This FDASIA Health IT Report focuses on a strategy and recommendations for the development of a regulatory framework for health IT. We note, however, that contractual limitations, fear of liability, and practices that discourage the free flow of information impede the development of a transparent learning environment. Examples like the the Patient Safety and Quality Improvement Act of 2005 have shown that liability laws that encourage stakeholders to behave in socially responsible ways and, where reasonably possible, mitigate significant risks to patient safety, may facilitate more rapid innovation, product enhancements, and improved patient safety.

Regarding listing, the IOM recommended that "all health IT vendors should be required to publicly register and list their products with ONC, initially beginning with EHRs certified for the meaningful use program" and that this should eventually include vendors of all health IT products. The FDASIA Workgroup also recommended that vendors should be required to list products which are considered to represent "at least some risk" if a "non-burdensome approach" can be identified.

Currently, ONC employs a mechanism for EHR developers to list their products that have been voluntarily tested and certified under the ONC Health IT Certification Program[61]. The listing includes the certifying body, original practice type, vendor, product, product version, product classification (e.g. "Complete EHR" or "EHR Module"), additional software required, and the voluntary certification criteria (including standards) to which the product was certified. The ONC Certified Health IT Product List is located at http://oncchpl.force.com/ehrcert.

Proponents of the requirement for health IT vendors to list selected health IT products with a centralized body contend that such an approach would improve transparency, promote safety, facilitate adverse event reporting and linking of adverse events to products, and serve as a resource for purchasers to know what products are available on the market. The Agencies agree that a voluntary, publicly accessible list of certain types of health management health IT products be maintained by a non-governmental program and made available to health IT consumers could provide additional consumer transparency and promote safety. Note, as most health management health IT, products, services, or systems are not devices, vendors, organizations, or individuals that manufacture such items are not required to register and list with FDA in accordance with section 510 of the FD&C Act.[62] In addition, if an item with health management health IT functionality meets the statutory definition of a device, FDA does not intend to focus its regulatory oversight on it.

The Health Information Technology Patient Safety Action & Surveillance Plan (Health IT Safety Plan)[63]

61 The Certified Health IT Product List provides the authoritative, comprehensive listing of Complete Electronic Health Records (EHRs) and EHR Modules that have been tested and certified under the ONC Health IT Certification Program. Each listed complete EHR and EHR module has been tested and certified by an authorized testing and certification body against applicable voluntary standards and certification criteria adopted by the HHS Secretary.

62 21 U.S.C. 360; see also 21 CFR part 807.

63 ONC, *Health Information Technology Patient Safety Action & Surveillance Plan*. July 2, 2013. Available at: http://www.healthit.gov/sites/default/files/safety_plan_master.pdf.

issued by ONC on behalf of HHS in July 2013 identified some immediate and short-term strategies and actions that HHS and stakeholders could take to improve health IT safety including but not limited to:

1) Increasing the quantity and quality of data and knowledge about health IT safety by facilitating reporting of patient safety events and unsafe conditions through the use of standardized formats for patient safety event reporting (such as the AHRQ Common Formats[64]) and the development of standardized mechanisms for reporting,[65] incorporating postmarket surveillance certification criteria for EHR technology, leveraging medical device health IT-related adverse event reports from FDA's Manufacturer and User Facility Device Experience (MAUDE) database and providing a mechanism through AHRQ's Network of Patient Safety Databases (NPSD) for aggregating and analyzing non-identified patient safety event information from multiple PSOs and other sources.[66]

2) Targeting resources and corrective actions to improve health IT safety and patient safety by working with private sector organizations that have the ability to investigate, take corrective action, and publicly report on their analysis of health IT-related hazards. For example, ONC has awarded a contract[67] to build upon The Joint Commission's existing sentinel events program to better identify, investigate, address, and educate stakeholders about the role of health IT as a cause of adverse events.

3) Promoting a culture of safety related to health IT by supporting the exchange of information about the safety of health IT products, consistent with reasonable intellectual property protections, cooperating on investigations and follow-up to identify and mitigate health IT-related problems, and accepting shared responsibility for systems interface and configuration.

ONC has established the Health IT Patient Safety Program to coordinate and implement the HHS Health IT Safety Plan in collaboration with federal partners. ONC also provides guidance for the safety-related surveillance of health IT certified under the ONC Health IT Certification Program.[68]

The FDA has taken numerous actions that can be leveraged to facilitate the creation of an environment of learning and continual improvement for health IT including:[69,70]

- Issuance of a road-map for the creation of a National Medical Device Postmarket Surveillance System that communicates timely, systematic, and prioritized device assessments using high quality, standardized, structured, electronic health-related data;
- Creation of a multi-stakeholder planning board to facilitate the creation of a sustainable, integrated medical device postmarket surveillance system;
- Establishment of a Unique Device Identification (UDI) System and creation of a publically accessible global UDI database to provide detailed, but not personally identifiable, device information to stakeholders and the general public;
- Piloting and planned deployment of the FDA Adverse Event Reporting System, a modernized database for adverse event reports; and
- Development of semantic text mining and automated adverse event review techniques to enhance identification of high-quality adverse event reports and trends.

For health IT to achieve its full potential to make health care safer, the public and private sector must work together to develop a culture of safety, transparency, learning, continual improvement, and shared responsibility with better-defined accountability. To encourage reporting, learning and improvement, the IOM, the FDASIA Workgroup, and many health

64 AHRQ maintains the Common Formats, a set of common definitions and reporting formats that allow health care providers to collect and submit standardized information regarding patient safety events and hazards, including those involving health IT. See AHRQ, *Common Formats* at http://www.pso.ahrq.gov/formats/commonfmt.htm.

65 See, for example, the Structured Data Capture Initiative within the Standards and Interoperability Framework at: http://wiki.siframework.org/Structured+Data+Capture+Initiative.

66 Network of Patient Safety Databases, http://www.pso.ahrq.gov/npsd/npsd.htm

67 Investigation of Health IT-Related Deaths, Serious Injuries, or Unsafe Conditions, Contract No. HHSP233201300019C.

68 ONC HIT Certification Program. Program Policy Guidance #13-01. Available at: http://www.healthit.gov/sites/default/files/onc-acb_2013annualsurveillanceguidance_final_0.pdf

69 Food and Drug Administration. Strengthening Our National System for Medical Device Postmarket Surveillance. September 2012. Available at: http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM301924.pdf.

70 Food and Drug Administration. Strengthening Our National System for Medical Device Postmarket Surveillance: Update and Next Steps. April 2013. Available at: http://www.fda.gov/downloads/MedicalDevices/Safety/CDRHPostmarketSurveillance/UCM348845.pdf.

IT stakeholders have advocated for a reporting environment that is non-punitive, arguing that disincentives to transparent reporting include fear of liability, punitive action, negative press or publicity, lack of trust, and fear of breaching confidentiality provisions of contracts with health IT vendors. To identify and monitor trends, identify underperforming products, mitigate future risk and facilitate improvement and learning, data analysis and reporting with transparency is necessary so that relevant findings from such analyses can be fed back into vendor and organizational risk management and quality systems programs.

The Agencies recommend the creation of a Health IT Safety Center. This public-private entity would be created by ONC, in collaboration with FDA, FCC, and AHRQ, and with involvement of other Federal agencies, and other health IT stakeholders. The Health IT Safety Center would serve as a trusted convener of stakeholders and as a forum for the exchange of ideas and information focused on promoting health IT as an integral part of patient safety. The Agencies believe this type of collaborative public-private effort is critical to the successful implementation of the strategy and recommendations contained in this report.

Summary and Conclusions

The public and private sector must work together to develop a culture of safety, transparency, learning, continual improvement, and shared responsibility with better-defined accountability. Vendors, health IT developers, health care providers and health care organizations should report serious health IT-related safety events to a trusted source that can aggregate and analyze information and disseminate findings. The Agencies recommend the creation of a public-private entity – the Health IT Safety Center - that would serve as a trusted convener of health IT stakeholders and identify the governance structures and functions needed for the creation of a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing and ongoing efforts.

The Agencies seek public input on the following questions related to creating an environment of learning and continual improvement:

- *What should be the governance structure and functions of the Health IT Safety Center, in order for it to serve as a central point for a learning environment, complement existing systems, facilitate reporting, and promote transparent sharing of adverse events, near misses, lessons learned, and best practices?*

- *How can comparative user experiences with health IT be captured and made available to the health IT community and other members of the public to promote learning?*

- *How can the private sector help facilitate the development of a non-governmental process for listing selected health IT products? What types of products and information should be included? Should the results of conformity assessments, such as conformance with certain clinical or privacy and security standards, be included?*

- *In terms of risk management, what type of safety-related surveillance is appropriate for health IT products categorized as health management functionality? What continued or expanded role(s), if any, should the ONC Health IT Certification Program play in the safety-related surveillance of health IT products?*

- *What role should government play in creating an environment of learning and continual improvement for health IT?*

6. ADDITIONAL CLARITY REGARDING CURRENT AGENCY FUNCTIONS

The FDASIA Workgroup recommended that additional clarity be provided regarding select current Agency functions and activities. Specifically, the Workgroup recommended that the following topics should be clarified through the development of draft documents and an open, collaborative process to engage public input: 1) the distinction between wellness and disease-related medical device claims; 2) medical device accessories; 3) clinical decision support software; 4) medical device software modules; and 5) inter-agency guidance on regulatory processes that affect manufacturers subject to FCC and FDA requirements.[71] We agree that additional clarity would be beneficial and note that actions 1), 2), and 4) pertain to all medical devices, not just medical device health IT. Prior to and independent of the statutory requirement to propose a regulatory framework for health IT and the development of recommendations by the FDASIA Workgroup, FDA had indicated that it would undertake some of these actions.

Clinical decision support (CDS) provides health care providers and patients with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care.[72] CDS encompasses a variety of tools intended to enhance, inform, and influence health care decisions. These tools include, but are not limited to, computerized alerts and reminders for providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; diagnostic support; and contextually relevant reference information. These functionalities can be deployed on a variety of platforms (e.g. mobile, cloud-based, installed).

CDS can contribute to increased quality of care and enhanced health outcomes, avoidance of errors and adverse events, improved efficiency, reduced costs, and enhanced provider and patient satisfaction. CDS is not intended to replace clinicians' judgment, but rather to assist clinicians in making timely, informed, higher quality decisions. Ultimately, the impact of CDS functionality on patient safety depends on the quality and reliability of the information and evidence, the analysis and customization underlying its implementation, and their transparency to users.

The following are examples of CDS that the Agencies recommend be categorized as health management health IT functionality for the purposes of this report's proposed framework. The Agencies believe that the non-regulatory approaches described in the health management health IT framework in Section 5 can be selectively applied to mitigate any safety risks posed by these functionalities. In applying a risk-based approach, FDA does not intend to focus its regulatory oversight on these products/functionalities, even if they meet the statutory definition of a medical device:[73]

- Evidence-based clinician order sets tailored for a particular condition, disease, or clinician preference;
- Drug-drug interaction and drug-allergy contraindication alerts to avert adverse drug events;
- Most drug dosing calculations;
- Drug formulary guidelines;
- Reminders for preventative care (e.g. mammography, colonoscopy, immunizations, etc.);
- Facilitation of access to treatment guidelines and other reference material that can provide information relevant to particular patients;
- Calculation of prediction rules and severity of illness assessments (e.g., APACHE score, AHRQ Pneumonia Severity Index, Charlson Index);
- Duplicate testing alerts;
- Suggestions for possible diagnoses based on patient-specific information retrieved from a patient's EHR.

71 Report of the Section 618 Regulations Subgroup – Summary. Available at: http://www.healthit.gov/facas/FACAS/health-it-policy-commitee/health-it-policy-committee-recommendations-national-coordinator-health-it (February 20, 2014).
72 See ONC, Clinical Decision Support at http://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds.
73 This is not intended to be an exhaustive list of all clinical decision support functionalities.

The FDASIA Workgroup and other health IT stakeholders have stated that some CDS software – those that are medical devices and present higher risks - warrant FDA's continued focus and oversight. Examples of medical device CDS currently regulated by FDA include but are not limited to:

- Computer aided detection/diagnostic software;
- Remote display or notification of real-time alarms (physiological, technical, advisory) from bedside monitors;
- Radiation treatment planning;
- Robotic surgical planning and control;
- Electrocardiography analytical software.

Consistent with the recommendation of the FDASIA Workgroup, FDA will work with federal and private stakeholders to clarify the types of medical device clinical decision support that should be the focus of FDA's oversight.

Clinical Decision Support

Summary and Conclusions

Most clinical decision support (CDS) functionalities can be categorized as health management health IT. FDA does not intend to focus its oversight on CDS with health management health IT functionality. Instead, the Agencies recommend that the four priority areas, identified in Section 5, should be selectively applied to mitigate the safety risks posed. In addition, the Agencies recommend that health IT stakeholders work together to develop policies for the transparent disclosure of the rules and information sources underlying individual health management CDS functionalities/products. For the small subset of CDS software that are medical device health IT functionality, present higher risks, and generally have been subject to active oversight by FDA, such active oversight should be continued. FDA will work with federal and private stakeholders to clarify the types of medical device clinical decision support that should be the focus of FDA's oversight.

The Agencies seek public input on the following questions related to clinical decision support (CDS):

- *What types of CDS functionality should be subject to the health management health IT framework? Which types should be the focus of FDA oversight?*

- *How should the following priority areas identified in the Health Management Health IT Framework (Section 5) be applied to CDS categorized as health management health IT functionality?*

    - *Quality Management Principles*
    - *Standards and Best Practices*
    - *Conformity Assessments*
    - *Learning Environment and Continual Improvement*

- *Are there additional safeguards for CDS, such as greater transparency with respect to CDS rules and information sources that are needed to appropriately balance patient safety and the promotion of innovation?*

- *Does the certification of CDS functionalities, such as those functionalities currently certified under the ONC Health IT Certification Program, sufficiently balance patient safety and the promotion of innovation?*

- *How can the private sector help assure the facilitation of the development, application and adoption of high quality CDS with health management health IT functionality in lieu of a regulatory approach? What role, if any, should government play?*

7. MECHANISM FOR CONTINUED AGENCY INTERACTIONS

FDA, ONC, and FCC have developed a collaborative, inter-Agency working group to support the development of this report and a health IT framework that promotes innovation, protects patient safety, and avoids regulatory duplication. We plan to continue working collaboratively and interactively on health IT-related activities to ensure an efficient, coordinated, transparent federal approach that actively engages and interacts with the stakeholder community on an ongoing basis. In order to accomplish this, we intend to take the following actions:

- Establish formal mechanisms and expectations for the three Agencies to continue to collaborate and interact;
- Coordinate with other Federal agencies involved in health IT; and
- Provide ongoing opportunities for feedback, input, and dialogue among health IT stakeholders and the FDA, ONC, and FCC.

7.1 Tri-Agency Collaboration

FDA, ONC, and FCC have long-standing, established mechanisms for collaboration, which will continue. For example, since signing a Memorandum of Understanding (MOU) in 2010, the FCC and FDA have conducted quarterly meetings and worked together to ensure that communications-related medical innovations can swiftly and safely be brought to market. FDA and FCC intend to continue to work together to clarify, and where possible, streamline regulatory processes that affect manufacturers subject to both FCC and FDA requirements. Similarly, ONC and FDA have an MOU to work together to help promote the safe adoption of health IT.

We intend to establish a tri-Agency MOU to clarify how we will exchange information with each other, discuss safety issues that may involve more than one agency, coordinate activities, and consider how the three Agencies will address new technologies and policies that are developed.

We also recognize that there are other Federal agencies that play an important role in facilitating the safe use of health IT and we have been actively engaged with many of them.[74] Other Federal agencies with public health, scientific, research, commerce, consumer protection and other expertise will continue to play an important role in promoting the safe development, implementation, and use of health IT. The Agencies also support ONC's plan to create an ad-hoc intra-departmental HHS multi-agency committee to address health IT safety issues that may arise and to share data about health IT safety. [75]

To provide clarity and to streamline the path to market for wireless medical devices with health IT functionality that currently undergo FDA pre-market review and FCC equipment authorization, the Agencies plan to seek public input from stakeholders to identify areas of potential overlap and opportunities for increased efficiency. Similarly, to identify tools and accelerate use of best practices in designing and implementing wireless health technologies that operate in potentially spectrum-crowded and interference-prone healthcare and home-based settings, the Agencies will collaborate to host a workshop on wireless test beds.

7.2 Ongoing Stakeholder Engagement

The Agencies recognize the importance of creating mechanisms for ongoing opportunities for feedback, input, and dialogue among health IT stakeholders, other federal agencies, FDA, ONC, and FCC. We plan to provide periodic tri-Agency reports to the ONC Health IT Policy Committee to communicate about Agency activities and to obtain input from the ONC Health IT Policy Committee and the public. We will also use additional mechanisms, as appropriate, for obtaining input, such as public meetings and requests for comment. Finally, the Agencies are requesting feedback on the strategy and recommendations for a risk-based regulatory framework for health IT proposed in this report. In addition, we will conduct a public meeting within 90 days of the report's release and prior to implementing the strategies and recommendations contained in this report.

74 See, for example, ONC, Health Information Technology Patient Safety Action & Surveillance Plan. July 2, 2013. Available at: http://www.healthit.gov/sites/default/files/safety_plan_master.pdf.
75 Ibid.

8. SUMMARY AND CONCLUSIONS

Health IT presents many new opportunities to improve patient care and safety. To promote innovation, protect patient safety and avoid regulatory duplication, the Agencies propose the creation of an agile, narrowly-tailored, risk-based health IT regulatory framework that primarily relies on ONC-coordinated activities and private sector capabilities, and focuses on health IT functionality rather than on the platform(s) on which it resides. We believe that active and ongoing stakeholder engagement is critical to the successful development and implementation of such a framework. After receiving public input and finalizing the proposed framework, the Agencies intend to continue active engagement with stakeholders in an ongoing collaborative effort to implement a health IT framework that promotes the electronic use and exchange of health information and helps the American public realize the tremendous potential benefits of health IT.

9. APPENDICES

9.1 Food and Drug Administration (FDA)

The FDA is an agency within the U.S. Department of Health and Human Services. FDA is responsible for protecting the public health by assuring the safety, effectiveness, quality, and security of human and veterinary drugs, vaccines and other biological products, and medical devices. The FDA is also responsible for the safety and security of most of our nation's food supply, all cosmetics, dietary supplements and products that give off radiation, and for regulating tobacco products.

Using the risk-based approach first established by the Medical Device Amendments of 1976[76], FDA has overseen medical devices[77], including "stand alone" and embedded medical device software, for close to four decades. The Agency has been regulating software on mobile platforms for more than a decade and has cleared for marketing approximately 100 mobile medical apps, including remote blood pressure, heart rhythm and patient monitors, and smartphone-based ultrasounds, electrocardiographic (ECG) machines and glucose monitors.

The FDA uses a targeted, focused approach to its oversight of "stand alone" medical device software that considers functionality rather than platform. FDA's guidance on Mobile Medical Applications announced a similar approach for this category of devices.[78] In this guidance, FDA also stated that the Agency does not regulate the sale or general consumer use of smartphones or tablets or consider entities that exclusively distribute mobile medical apps, such as the owners and operators of the "iTunes App store" or the "Android market," to be medical device manufacturers. Nor does the Agency consider mobile platform manufacturers to be medical device manufacturers just because their mobile platform

76 The Medical Device Amendments of 1976 created three device classes. The three classes are based on the degree of control necessary to assure that the various types of devices are safe and effective. **Class I** devices are generally low risk. Such devices are for the most part exempt from premarket review and are subject –unless exempt – to the requirements for reporting of adverse events, manufacturing and design controls, registration and listing, and other "general" controls. **Class II** devices generally present moderate or well-understood risks. Such devices are subject to general controls and are usually subject to premarket review. Class II devices are also subject to "special controls" that are closely tailored to the risks of the particular device type. **Class III** devices generally present high or poorly understood risks. In addition to general controls, Class III devices are subject to premarket approval and certain other regulatory controls.

77 Products that are built with or consist of computer and/or software components or applications are subject to regulation as devices when they meet the definition of a device in section 201(h) of the FD&C Act. That provision defines a device as "…an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory", that is "… intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man…" or "… intended to affect the structure or any function of the body of man or other animals …." Thus, software applications that run on a desktop computer, laptop computer, remotely on a website or "cloud," or on a handheld computer may be subject to device regulation if they are intended for use in the diagnosis or the cure, mitigation, treatment, or prevention of disease, or to affect the structure or any function of the body of man. The level of regulatory control necessary to assure safety and effectiveness varies based upon the risk the device presents to public health.

78 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. September 25, 2013. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

could be used to run a product regulated by FDA. In addition, FDA's regulations, guidance, and policies do not require medical device software developers to seek Agency re-evaluation for minor, iterative product changes that do not affect the safety or effectiveness of the device.

Additional information about FDA's regulation of medical devices can be found at:

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/default.htm.

9.2 Office of the National Coordinator for Health Information Technology

The Office of the National Coordinator for Health Information Technology (ONC) was created within the Department of Health and Human Services (HHS) first by Executive Order 13335 on April 27, 2004[79] and then through the Health Information Technology for Economic and Clinical Health (HITECH) Act passed as part of the American Recovery and Reinvestment Act (Recovery Act) of 2009.[80] Section 3001 of the Public Health Service Act (PHSA) as added by HITECH, provides the National Coordinator for Health Information Technology ("National Coordinator") with additional responsibilities and duties beyond those originally identified in Executive Order 13335. The National Coordinator is charged with, among other duties: reviewing and determining whether to endorse each standard, implementation specification, and certification criterion that is recommended by the Health IT Standards Committee (a federal advisory committee to the National Coordinator) and making such determinations and reporting them to the Secretary; reviewing Federal health IT investments to ensure that they meet the objectives of the Federal Health IT Strategic Plan; coordinating the health IT policy and programs of HHS with those of other relevant Federal agencies; serving as a leading member in the establishment and operations of the Health IT Policy Committee (a federal advisory committee to the National Coordinator) and Health IT Standards Committee; updating the Federal Health IT Strategic Plan in consultation with other appropriate Federal agencies and through collaboration with public and private entities; keeping or recognizing a program or programs to certify EHR technology; conducting studies and issuing reports; and establishing a governance mechanism for the nationwide health information network.

ONC has focused many of its efforts to date on the adoption and certification of EHR technology, the interoperable and secure electronic exchange of health information, promoting patient access to their electronic health information, and coordinating health IT efforts across the Federal government through the Federal Health IT Strategic Plan.

Certification Authority

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, PHSA section 3001(c)(5)(A) specifies that the "National Coordinator, in consultation with the Director of the National Institute of Standards and Technology, shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle" (i.e., certification criteria adopted by the Secretary under section 3004 of the PHSA). ONC relied upon this authority to establish the ONC Health IT Certification Program. EHR technology is currently certified under this program as either a Complete EHR or EHR Module for either the ambulatory or inpatient setting. While ONC has focused on EHR technology certification, it also has authority to certify other types of health IT. [81]

Understanding Health IT Safety

Health IT presents new opportunities to improve patient care and safety, through better access to patient information, decision support, and population

79 Exec. Order No. 13335, 69 Fed. Reg. 84, 24059 (April 30, 2004) ("The National Coordinator shall [coordinate the development and implementation of] interoperable health information technology.").

80 Health Information Technology for Economic and Clinical Health (HITECH) Act. Pub. L. 111-5, 123 Stat. 115, Division A, Title XIII & Division B, Title IV. The HITECH Act directs the National Coordinator to coordinate the development of a nationwide health IT infrastructure that, *inter alia*, "reduces medical errors" and "improves health care quality." 42 U.S.C. § 300jj-11(b).

81 Health Information Technology for Economic and Clinical Health (HITECH) Act. Public Law 111-5, February 17, 2009. 123 STAT 232.

information. It is also true that any new technology comes with new potential hazards. Health IT can only fulfill its potential to improve patient safety if the risks associated with its use are identified, if there is a coordinated effort to mitigate those risks, and if it is used to make health care safer. With those challenges in mind, ONC commissioned the Institute of Medicine (IOM) to study and report on health IT and patient safety, and IOM produced a report in November 2011 entitled, *Health IT and Patient Safety: Building Safer Systems for Better Care*.

In response to this report, ONC took two significant steps: 1) ONC proposed and adopted certification criteria for EHR technology, under the ONC HIT Certification Program, focused on safe EHR technology design; and 2) ONC published the *Health IT Patient Safety Action and Surveillance Plan* (the "Health IT Safety Plan")[82], which addresses the role of health IT within HHS's overall commitment to patient safety.

Building on the IOM's recommendations, the Health IT Safety Plan leverages existing authorities to strengthen patient safety efforts across government programs and the private sector—including patients, health care providers, technology companies, and health care safety oversight bodies. Importantly, the Health IT Safety Plan outlines specific and tangible actions through which all stakeholders can fulfill their shared obligation to increase knowledge of the impact of health IT on patient safety, and maximize the safety of health IT and health IT-assisted care. These actions focus on learning more about the risks associated with health IT, improving the development and implementation of health IT to promote safety, and leading a coordinated effort by the public and private sectors to create a culture of safety. Since the publication of the Health IT Safety Plan, ONC has, among other things:

- Published the Safety Assurance Factors for EHR Resilience (SAFER) Guides, which are self-assessment guides with recommended practices in nine areas designed to optimize the safety and safe use of health IT; and
- Initiated activities to create the Health IT Safety Center, which it expects to launch in 2014.

9.3 Federal Communications Commission

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. It was established by the Communications Act of 1934 and operates as an independent U.S. government agency overseen by Congress. The Commission is committed to being a responsive, efficient and effective agency capable of facing the technological and economic opportunities of the new millennium. In its work, the Commission seeks to capitalize on its competencies in:

- Promoting competition, innovation, and investment in broadband services and facilities;
- Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution;
- Encouraging the highest and best use of spectrum domestically and internationally;
- Revising media regulations so that new technologies flourish alongside diversity and localism; and
- Providing leadership in strengthening the defense of the nation's communications infrastructure.

The FCC oversees the authorization of equipment using the radio frequency spectrum. These devices may not be imported and/or marketed until they have shown compliance with the technical standards specified by the Commission. These standards are found in the rules that govern the service where the equipment is to be operated. The FCC is also responsible for governing the interference potential of equipment which emits radio frequency energy. It does this by first establishing technical regulations for transmitters and other equipment to minimize their potential for causing interference to radio services, and then administering an equipment authorization program to ensure that equipment reaching the market complies with the technical requirements. The equipment authorization program requires that equipment be tested to ensure that it complies with the technical requirements prior to marketing.

The FCC is committed to accelerating the adoption of

82 ONC, *Health Information Technology Patient Safety Action & Surveillance Plan*. July 2, 2013. Available at: http://www.healthit.gov/sites/default/files/safety_plan_master.pdf.

health care technologies to improve health outcomes and lower health care costs. FCC works closely with FDA and other public and private stakeholders. In 2010, the FCC entered into an unprecedented partnership with the FDA for the Agencies to work together to ensure that communications-related medical innovations can swiftly and safely be brought to market. In addition, in June 2012, the FCC worked with an independent mHealth[83] Task Force, which collaborated on several policy recommendations to the FCC, other Federal agencies, and to industry, with the goal of making mHealth a routine medical best practice by 2017. To date, FCC has acted on nearly all of the mHealth Task Force's recommendations including actions to increase interagency collaboration and information sharing, expand on existing programs to encourage mHealth adoption, and build on government and industry efforts to increase capacity, reliability, interoperability, and safety of mHealth technologies. The FCC has recently established a health subcommittee for its Consumer Advisory Committee (a federal advisory committee), chaired by the leaders of the mHealth Task Force and has held an mHealth Innovation Expo at its headquarters.

The FCC's Office of Engineering and Technology (OET) manages spectrum and works to create new opportunities for competitive technologies, including wireless medical devices. OET conducts many activities relating to wireless medical devices, including equipment authorization (for products such as smartphones, wi-fi devices, and personal computers); testing for radio frequency safety; and regulation of radio spectrum. Some examples of recent FCC actions include:

- MedRadio (Medical Device Radio communications Service): In the course of two rulemaking proceedings, the Commission allocated spectrum and adopted technical rules for innovative new body-worn and implanted medical radio devices that can perform a variety of diagnostic and therapeutic functions from glucose and heart monitors to pacemakers and cardiac defibrillators.

- Medical Body Area Networks (MBANs): In 2012, the FCC released an Order to allocate spectrum for Medical Body Area Networks (MBANs), making the U.S. the first country in the world to make spectrum available for this specific usage. MBANs are networks of wireless sensors, often no bigger than a band-aid, which can transmit data on a patient's vital health indicators to their doctor or hospital.

- Medical Micropower Networks (MMNs): In 2011, the FCC adopted rules to enable a new generation of wireless medical devices that can be used to restore functions to paralyzed limbs. MMNs are ultra-low power wideband networks consisting of transmitters implanted in the body that take the place of damaged nerves, restoring sensation and mobility.

- Experimental Licensing Program: In May 2012, the FCC announced a plan to cut red tape and increase spectrum flexibility for testing new wireless health innovations, to speed new wireless health technologies to market. The new experimental licensing regime will create more flexibility and streamlined processes for testing new wireless medical devices. Specifically, through a "medical testing license," qualified healthcare facilities would have broad authority to conduct research without the need to seek new approval for each individual experiment. FCC's Experimental Licensing Program will become operational in 2014 and will help facilities, and industry more broadly, better evaluate

83 While mHealth traditionally stands for "mobile health," the mHealth Task Force adopted the term more broadly to refer to mobile health, wireless health, and e-Care technologies that improve patient care and the efficiency of healthcare delivery. See mHealth Task Force: Findings and Recommendations at: http://transition.fcc.gov/cgb/mhealth/mHealthRecommendations.pdf

how wireless technologies and other electronic devices coexist in a hospital environment (http://www.fcc.gov/health#oet).

The Enforcement Bureau (EB) is the primary FCC unit responsible for enforcing the provisions of the Communications Act and the Commission's rules, orders, and various licensing terms and conditions. EB's mission is to investigate and respond quickly to potential unlawful conduct to ensure: (1) consumer protection in an era of complex communications; (2) a level playing field to promote robust competition; (3) efficient and responsible use of the public airwaves; and (4) strict compliance with public safety-related rules.

The Commission and its EB enforce the Communications Act and the Commission's rules and orders in two primary ways: (1) by initiating investigations, and taking appropriate action if violations are found; and (2) by resolving disputes between industry participants either through mediation and settlement, or adjudication of formal complaints.

Food and Drug Administration
Center for Devices and Radiological Health
10903 New Hampshire Avenue
Silver Spring, MD 20993
http://www.fda.gov/MedicalDevices
http://www.fda.gov/Radiation-EmittingProducts

Federal Communications Commission
445 12th Street SW, Washington, DC 20554
ttp;// http://www.fcc.gov/

The Office of the National Coordinator for Health Information Technology
200 Independence Avenue, S.W. Suite 729D Washington, D.C. 20201
http://www.healthit.gov/