**Summary/Highlights of**

**FDASIA Request for Comment (RFC)**

**on the Development of a Risk-Based Regulatory Framework and Strategy**

**for Health Information Technology**

**78 FR 32390 (May 30, 2013)**

1. Comments are due by August 31, 2013.
2. Comments were requested by ***June 30, 2013***, for consideration by the HIT Policy Committee FDASIA Workgroup.

**Taxonomy**

***a. What types of health IT should be addressed by the report developed by FDA, ONC, and FCC?***

**Review the full range of health IT products and carefully judge the extent to which they pose risk to patients. Doesn’t mean all types have to be regulated.**

Supported by: AHA, EHRA, MITA, athenahealth, and generally by other commenters.

**BPC Report (medical device software, administrative software, and clinical software)**

Supported by: AMIA, EHRA, McKesson Corp., Greenway Medical Technologies, athenahealth, and MITA (not a listed BPC Report contributor).

**Codenomicon**

Recommends addressing: all healthcare systems and devices which communicate over any communication channel (wired or wireless); the methodologies used to evaluate vulnerabilities in the systems and devices from a functional and non-functional perspective; the qualifications of the personnel the manufacturers, integrators, and end users of systems and devices use to determine the vulnerabilities found in the systems and devices; and the qualifications of the personnel the manufacturers, integrators, and end users of systems and devices use to determine the design criteria for securing the systems and devices.

**Verizon**

* FDA should focus and narrow its interpretation of the types of products that fall within the definition of medical devices by limiting regulation to products that diagnose or treat disease.
* FDA should ***not*** focus on products that "provide patient-specific medical device data especially when the patient-specific information is reviewed by a physician or other learned intermediary as only one of potentially many sources of information. Application of the medical device definition to these products should be as narrow as possible for health care devices that present low or minimal risk of harm to users.

**Pharmacy e-HIT Collaborative**

Mobile medical devices and mobile medical apps

**AMIA**

* Recommends adopting consistent terminology for terms such as “electronic health records (EHRs)”, “personal health records (PHRs)”, “mobile apps”, “telehealth”, “telemedicine”, “m-health”, “patient-managed tools” (e.g., PatientsLikeMe) and other forms of health IT.
* Define clinical decision support (CDS) software to support efforts to “identify and distinguish what types of software should potentially be regulated as a medical device, and which software should not. See AMIA 2006 “Roadmap” produced with funding from ONC and AHRQ. AMIA consider CDS software to be any application which brings relevant clinical data and knowledge together to improve clinical decision making by either care providers or patients.
* HHS should consider distinctions between mobile apps that stand alone from those that allow access to larger systems, such as EHRs or health information exchanges (HIEs).
* Recommends that consumer-oriented health IT devices and applications (such as those which do not provide data directly to the individual’s EHR) should not be directly regulated.
* Recommends establishing use cases (articulation of use cases will facilitate the development and validation of standardized performance measures for assessing the incidence of adverse events and medical errors.)

**AdvaMed**

* Regulation of Health IT (which encompasses software) should be platform agnostic.
* Health IT should be handled similarly to other FDA-regulated medical devices. If it meets that definition, it should be regulated using the same risk classification and safety and efficacy schema as any other medical device.

**MITA**

Proposes the definition of HIT as follows: “*Health Information Technology (HIT) is software and its hardware and process dependencies used in the healthcare sector that have an impact on the health and healthcare of its subject(s). Dependencies include the network and end user equipment, and process refers to the elements such as the use, configuration, and customization.”*

**athenahealth**

* The formerly-reasonable distinction between “mobile” information technology and “other” is more a fiction with every passing day. Any regulatory regime that seeks to regulate “mobile” separately from or differently than other forms of information technology will be obsolete soon after (if not before) promulgation.
* Avoid prescriptions based on current technology, or even on assumptions about where innovation will take health IT next. Focus on what the technology *does*, rather than on current conceptions of what the technology *is* (*e.g*., mobile, static, cloud-based, etc.).

**PhRMA**

Prove a clear definition of types of HIT covered.

**eHealth Initiative (eHI)**

* Focus of the report should not be placed upon what “types of health IT” should be addressed but rather placing an emphasis on the broader scope of health IT that includes the full range of tools and applications across the risk spectrum and their impact on patient safety, including those currently regulated by the FDA.
* As the patient safety framework is developed, we strongly urge consideration of the software and use of technology that accomplishes the process of exchanging health information, which may occur as part of or outside of a formal HIE organization. We believe the inclusion of an HIE *organization* falls outside the scope of this effort and suggest the act of exchanging information and mitigating risk factors within HIE organizations should be addressed within the patient safety framework.

**Risk and Innovation**

***a. What are the risks to patient safety posed by health IT and what is the likelihood of these risks?***

**McKesson Corp.**

* See BPC Report
* The recent *ECRI PSO Deep Dive Report* on health IT illustrates that a significant contributing factor to patient safety is system configuration and use, a finding that is consistent with the 2012 Institute of Medicine study. During the FDASIA workgroup’s public meeting on May 30, 2013, several examples of health IT risks were presented and discussed in which the initiating event originated with the configuration of medical devices currently regulated by the FDA. Date and time settings and data sampling intervals were incorrect, which presented a risk to the patient. In the current model that FDA uses for regulation of medical devices, neither of these risk factors would be considered. This deficiency further underscores the need for a safety assessment of health IT that includes oversight of its implementation, configuration and use.

**Athenahealth, EHRA**

Cites IOM review of seven papers finding that health information systems were involved in less than 1 (one) percent of reported errors.” (Also cites to Pennsylvania PSA report and note cross-references to ONC Safety Plan).

**EHRA**

It is helpful to look to the National Quality Strategy, the Partnership for Patients, CMS actions around safety, state efforts, the Joint Commission, and Patient Safety Organizations (PSOs) for information about patient safety risks. The Association supports additional efforts to review patient safety reporting information to evaluate the role of health IT in these reported incident.

**AMIA**

Usability issues can adversely affect patient safety and the quality of care.

**AHA**

* In looking at specific products, attributes such as safe design, use of quality management principles, user-centered design and human factors assessments have been shown to improve safety. Therefore, the agencies should look carefully at the interaction between usability of health IT products and patient safety.
* The general inability of systems to easily share data using the same set of standards (interoperability) also can pose safety risks.
* Incorrect patient matching

**eHealth Initiative (eHI)**

Recognize that the use of health IT, can, in some instances, poses risks to patients; for example, there have been published examples of accidently transposing values and numbers and medication measurement errors. Other factors such as provider workflow, usability, and the way in which health information is leveraged is an important strategy for mitigating patient safety risks and thus requires further analysis.

**Codenomicon**

Any device which communicates over a wired or wireless channel poses a risk (equivalent to 100%) that either a malicious actor or curious explorer will access and potentially cause harm to the patient it is being used on.

***b. What factors or approaches could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety?***

**BPC Report (also consider cost and burden of regulation)**

Supported by: EHRA, Greenway Technologies, McKesson Corp., MITA, AMIA (see also Safety Plan and Mobile Apps submissions), athenahealth, and Pacific Northwest National Laboratory.

**Use existing voluntary safety reporting systems**

Supported by: AMIA (see also AMIA Task Force Report), EHRA, AHA, MITA, andeHealth Initiative (eHI).

* Voluntary provider reporting to PSOs on safety issues should be the primary focus, given that safety events generally happen in a provider context and that health IT is likely to be only one element of any safety event. **Generally all specified commenters.**
* Consider utilizing accrediting bodies, state and national level mandatory reporting, and CDC required reporting. **eHealth Initiative (eHI)**
* Leverage the AHRQ Network of Patient Safety Databases for aggregation and high-level analysis of safety reports. **EHRA**

**Use consensus-based, nationally or internationally recognized standards**

Supported by: AvaMed, MITA, Verizon, McKesson Corp., and Pharmacy e-HIT Collaborative.

* For example: ISO 25238, ISO 14971, IEC 62304, and IEC/TR 80002-1, and ANSI supported standards.

**Security testing**

Supported by: AHA, AMIA, and Codenomicon.

* A thorough vulnerability assessment which includes the following: Fuzz testing of all communication protocols; hardware security analysis; factory acceptance testing; interoperability testing; sight acceptance testing; code signing of all binaries used in medical devices; and failure mode effects of fuzz testing and fault injections. It is extremely important to note that most design processes focus on testing of functional requirements. Most vulnerabilities discovered are the result of non-functional use (or negative testing) of devices. Most medical manufacturers and end users are not equipped with tools to perform these types of tests. Other industries perform such tests as a normal part of development, using COTS tools and software. **Codenomicon**

**Pharmacy e-HIT Collaborative**

Producers of mobile medical devices and mobile medical apps should be encouraged to certify that their products follow and meet acceptable HIT standards and platforms for the collection, exchange, and protection of patient health information, as well as ensuring patient safety and well-being in the use of these devices and information to support positive health outcomes.

**AdvaMed**

Historically, a leading inhibitor of medical device innovation has been the lack of global harmonization of regulatory requirements. This lack of global regulatory harmonization may force country-specific verification and validation activities and lifecycle management decisions, which is both costly and complex. This cost and complexity can easily stifle innovation.

**AHA**

* Key factors to be considered include the potential for harm, the extent of harm, and the extent to which software is automating and or guiding clinical decision-making. Agencies also should consider the extent to which a product is transforming data points (such as laboratory values or drug dosages) used to guide clinical decision-making and treatment. For example, when drug dosage data are sent from an order entry system to a pharmacy information system, it is crucial for safety that both the data points and their units of measure are accurate within each system and across systems.
* Manufacturers should not be allowed to include in their contracts indemnity clauses or nondisclosure language that limits the ability of users to identify and publicly raise safety concerns.
* Consider the safety issues that stem from the lack of a single, national approach to matching patients to their records that all parties can use to accurately and efficiently exchange health information.

**EHRA and Greenway Medical Technologies**

Sees little benefit from:

* Using meaningful use regulations and certification to embed intrusive requirements into EHR design that are not conducive to or needed for a learning system;
* Expanding the role of the ONC Authorized Certification Bodies (ACBs) role into patient safety evaluation and enforcement, which is not within their core competencies;
* Equating usability with patient safety. Although some usability issues may affect safety, we do not agree that comparing users’ experiences can determine safety among EHRs. We suggest that it is more appropriate to implement evaluation processes such as reporting, analyzing, and learning to determine the impacts of health IT and usability on patient safety, before devising a regulatory or oversight approach to usability.

**Verizon**

* Utilize existing exemptions (and create new exemptions) to premarket application filing and manufacturing quality system regulations ("QSRs") available to particular Class I and Class II devices; and/or (3) apply enforcement discretion, a regulatory practice whereby FDA purposefully declines to exercise its full regulatory and enforcement authority with respect to products and solutions despite apparent jurisdiction to do so, in cases where there is minimal potential risk of patient harm.
* Use narrow medical device interpretation as noted in “Taxonomy” response or regulated medical devices in this field should be classified as Class I exempt from 510(k)s, pre-market approval, and QSRs if they are unlikely to cause patient harm. When the FDA deems a medical device to pose little or no potential for patient harm, or if the use of the device is well-documented and understood, the FDA could classify such a device as Class I exempt. Such an exemption could apply initially to the filing of premarket approval applications and compliance with QSR. FDA could adjust this approach, if justified, based on its monitoring of the performance of these devices and the filing of any Medical Device Reports (MDRs). An exercise of enforcement discretion by FDA's CDRH may be required and appropriate in certain cases, such that FDA would decline to pursue enforcement action for violations of the Act, including allowing a product to remain on the market that FDA believes is within the definition of a medical device, but for which premarket approval has not been sought. Enforcement discretion for low-risk devices with respect to compliance with QSR could encourage development of meaningful new technologies and applications. This would alleviate the concern of manufacturers whose core technologies are not usually subject to FDA regulatory authority, that their operations would fall within the burdensome FDA QSR regime. It may be appropriate for FDA to establish a policy, in conjunction with its exercise of enforcement discretion, which would provide application developers and others a specific period of time in which to come into compliance with the waived requirements if an exercise of enforcement discretion is rescinded.

**eHealth Initiative (eHI)**

* Evaluate the available peer reviewed and other high quality literature on benefits and risks associated with health IT, including incidence and prevalence.
* Focus on the potential that a technology or product can cause harm, the likelihood that such potentially harmful situations will occur, the extent of harm, and the extent to which the risk can be mitigated or not, for example whether the technology guides clinical decision-making without clinician intervention. A risk based framework should allow for the appropriate level of oversight or regulation, and should also consider the costs and benefits of regulation or oversight and support the continuation and flexibility of innovation of health IT.

**Regulation**

***a. Are there current areas of regulatory overlap among FDA, ONC, and/or FCC and if so, what are they? Please be specific if possible.***

**Conduct an environmental scan of existing regulatory efforts as context for the report**

Supported by: AHA, eHealth Initiative (eHI), and AMIA.

* Seek to minimize duplicative, or worse, conflicting regulations. The hospital field is highly regulated by federal, state and local governments, and includes many private sector activities aimed to ensure and enhance patient safety. These include, but are not limited to, Medicare’s conditions of participation, accreditation by The Joint Commission or other federally recognized entities (which includes extensive analysis of health information and record management), Centers for Medicare & Medicaid Services requirements for hospital laboratories (including lab information systems), state licensure of hospitals and health care providers, certifications from professional societies and many other ongoing activities. **AHA**
* Encourage the inclusion of existing national, state, and local regulations to prevent duplicative and/or conflicting efforts. **eHealth Initiative (eHI)**

**PhRMA**

Redundancy w/n FDA – no clear policies between centers (CDER, CDRH, and CBER)

**EHRA, Greenway Medical Technologies**

There exists some levels of uncertainty regarding FDA plans for EHRs, mobile applications and clinical decision support. There is also growing FCC interest in aspects of mobile healthcare devices. In some cases, the same solution might be subject to multiple regulatory approaches, especially regarding aspects of patient safety. In other cases, the same company might be subject to overlapping regulations by virtue of its range of offered solutions. In still others, two different agencies can require or reference use of the same type of safety function, such as quality management systems. Additionally, there are many programs both public and private that create quasi-regulatory obligations on health IT, including patient safety and adverse event reporting, Medicare and Medicaid conditions of participation, provider quality reporting and more.

**MITA**

Potential regulatory overlap, for example, could arise with respect to regulation of “security” issues as these agencies are becoming increasingly engaged with regulation of cyber-security issues. We do not believe that such overlap can or should be entirely eliminated but it must be minimized and managed carefully to avoid duplication.

**McKesson Corp.**

* Regulatory overlap exists today. Section 201(h) of the Federal Food, Drug and Cosmetic Act gives the FDA the authority to regulate “medical devices” under a definition that was adopted in the 1970s. Under this broad definition, medical software could be subject to regulation as a medical device; concurrently it must also meet certification and content standards established by the ONC as part of the Meaningful Use program.
* Notes all the actions by FDA, ONC, and FCC, has led to public confusion over who will ultimately have jurisdiction over health IT and the electronic transmission of health information.
* Overlap on QMS with FDA and the ONC HIT Certification Program.

**athenahealth**

Suggests it is unclear where these two agencies are headed and overlap concern. Points to the Health IT Patient Safety Action and Surveillance Plan and a FDA-issued “safety communication,” warning of potential computer virus threats associated with the use of medical technology.

***b. 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?***

**Clarify agency roles and avoid overlap**

Supported by: EHRA, Greenway Medical Technologies, AHA, AMIA, MITA and Verizon.

* Multiple federal regulatory agencies (e.g., FDA, ONC, FCC, CMS, OCR, etc.) have overlapping, complementary, parallel, or similar health IT regulations, for example, the CMS and ONC meaningful use regulations. There also needs to be an effective “single source of truth” across all regulatory agencies to ensure that regulations are clear, unambiguous, and which do not collide or conflict with other regulations or reporting requirements. We therefore recommend that agencies develop a consistent format for the industry to access (via the Web) the current laws, regulations, and guidance, including FAQs. Each of these agencies now has its unique design, navigation, and search capabilities for their websites which hinders industry access and makes the task of locating and understanding the latest information more difficult and subject to error. **EHRA, Greenway Medical Technologies**
* Delineate and maintain separate focuses of agencies (ONC on privacy and security and infrastructure and FDA on public health and safety) **PhRMA**
* Several key issues need to be considered, such as: If there are safety aspects of certification, should FDA take that over? For example, in the 2014 Certification Criteria, there are usability requirements. Such requirements are likely to grow over time; however it is not clear the extent to which FDA or ONC should be responsible for assessing those requirements. Although AMIA believes that in the near term, it would make sense for ONC to keep responsibility for the safety aspects/components of EHR certification criteria; this may need to be reassessed in the future. **AMIA**

**Quality Management Systems - Should allow manufacturers to apply a single process that satisfies the requirements of all agencies.**

Supported by: MITA, eHealth Initiative (eHI), and AMIA.

**Conduct outreach**

Supported by: AHA, MITA, eHealth Initiative (eHI), and AMIA.

* Ongoing development and dissemination of best practices in the safe design, development, deployment and use of EHRs would be helpful. **AHA and AMIA**
* Conduct town hall meetings and forums for more public input. **eHealth Initiative (eHI)**

**PhRMA**

Avoid impeding the EHR Incentive Programs which are leading to the adoption of HIT that can improve patient safety.

**AMIA**

* FDA, ONC and FCC should consider establishing a standing working group that includes personnel from each of these and other agencies, as well as subject matter experts from the private sector in technology, informatics, computer sciences, consumer protection, and other disciplines, to provide continuing input to a regulatory framework that will evolve.

**McKesson Corp.**

* ONC is well positioned to oversee and promote health IT safety.
* A new framework is needed to promote both continuous quality improvements in patient safety as well as ongoing innovation in the development of health IT.
* See also BPC Report.

**Verizon**

* Recommends coordination among agencies, including issues connected to the Universal Service Rural Health Care Fund
* Adopt a series of MOUs on minimizing and/or eliminating regulatory overlap.
* Create an FDA office, working group, or task force for mobile health.