A risk-based regulatory framework for health IT: recommendations of the FDASIA working group

Sarah P Slight,[1,2] David W Bates[2,3,4]

[1]Division of Pharmacy, School of Medicine, Pharmacy and Health, The University of Durham, Stockton-on-Tees, UK
[2]Department of Medicine, Brigham and Women's Hospital, Boston, Massachusetts, USA
[3]Harvard Medical School, Boston, Massachusetts, USA
[4]Department of Health Policy and Management, Harvard School of Public Health, Boston, Massachusetts, USA

Correspondence to
Dr David Westfall Bates, Division of General Internal Medicine, The Center for Patient Safety Research and Practice, Brigham and Women's Hospital, 1620 Tremont St, Boston, MA 2120, USA; dbates@partners.org

Received 8 January 2014
Revised 7 April 2014
Accepted 8 April 2014
Published Online First 24 April 2014

ABSTRACT

The Secretary of Health and Human Services (HHS) acting through the Food and Drug Administration (FDA), and in collaboration with the Federal Communications Commission (FCC) and Office of the National Coordinator for Health IT (ONC) was tasked with delivering a report on an appropriate, risk-based regulatory framework for health information technology (IT). An expert stakeholder group was established under the auspices of the Health IT Policy Committee to help provide input into the development of this framework, including how healthcare IT systems could be stratified in terms of risk and recommendations about how the regulatory requirements currently in place should be adapted. In this paper, we summarize the public deliberations and final public report of the expert stakeholder group, and conclude with key suggestions intended to address the charge to recommend the features of a risk-based regulatory framework that promote innovation, protect patient safety, and avoid regulatory duplication.

INTRODUCTION

On July 9, 2012, President Barack Obama signed into law the Food and Drug Administration Safety and Innovation Act (FDASIA).[1] This legislation enhanced the powers of the Food and Drug Administration (FDA) to protect and promote patients' interests by expediting the development and review of new medical devices. The Secretary of Health and Human Services acting through the FDA, and in collaboration with the Federal Communications Commission (FCC) and Office of the National Coordinator for Health Information Technology (ONC), was tasked with delivering a report that contained 'a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology (IT), including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication.'[1] Recognizing the importance of stakeholder involvement, the FDA set up the public–private FDASIA working group under the ONC's Health IT Policy Committee.[2] The purpose of this group, which was subject to Federal Advisory Committee regulations, was to gather expert input from a wide variety of relevant stakeholders including patients, consumers, healthcare providers, and IT vendors, to help guide the FDA on the development of such a framework. The group was keen to avoid any regulatory duplication, as a number of different organizations are already responsible for assuring the safety and effectiveness of medical devices (FDA), and testing and certifying of products (ONC). With publication of this health IT report now imminent, we reflect on the key recommendations of the FDASIA working group that were made in response to this charge, as well as identify the actions necessary to make the risk-based regulatory framework work without stifling innovation.

WHAT HEALTH IT SHOULD BE SUBJECT TO A RISK-BASED REGULATORY FRAMEWORK?

The FDASIA working group described a taxonomy for considering the parameters of health IT and consequently what health IT products should be considered for a risk-based regulatory framework.[3] A number of guiding principles were intended to be applied to these health IT products, including a set of defining characteristics such as product categories and intended use. If the intended use of the health IT product was to inform or change decision making about initiating, discontinuing, modifying, or avoiding care interventions or personal health management, then it was considered within the scope of the framework. Electronic health records (EHRs), intelligent intravenous (IV) pumps, closed-loop insulin pumps with implanted continuous glucose monitors, and an mHealth nutrition app were all given as examples of health IT products that could possibly be subject to a risk-based regulatory framework, whereas disease registries and claims processing software were considered out-of-scope (table 1).

HOW CAN HEALTH IT BE STRATIFIED IN TERMS OF RISK?

The FDASIA working group developed a new framework enumerating various important factors that could influence the potential risk of patient harm (combination of the probability of occurrence of harm and the severity of that harm). These included, for example, the purpose of the software product, intended user(s), severity of injury, likelihood of hazardous situation arising, and complexity of implementation and upgrades (see table 2). The framework did not weight or 'calculate' any specific risk score for a given product, but rather served to highlight the key considerations when evaluating the use of a new system. The matrix characterized the relative risk (ie, 'lower risk,' 'medium risk,' or 'higher risk') of certain conditions of each risk factor and served as directional guidance only. Software may be considered complex in terms of implementation, upgrades, and maintenance, and thus harder to classify. This is somewhat understandable given: (i) the greater effort and expertise required to implement software, (ii) the variable context of use, and (iii) the existence of numerous interfaces to other systems.

To cite: Slight SP, Bates DW. *J Am Med Inform Assoc* 2014;**21**:e181–e184.

Table 1 Examples of health IT products that may or may not be possibly subject to the risk-based regulatory framework[3]

Possibly subject to risk-based regulatory framework	Likely *not* to be subject to the risk-based regulatory framework
EHRs (installed, SaaS)	Claims processing software
Hospital information systems-of-systems	Health benefit eligibility software
Decision support algorithms	Practice management/scheduling/ inventory management software
Visualization tools for anatomical tissue images, medical imaging, and waveforms	General purpose communication applications (eg, email, paging) used by health professionals
Health information exchange software	Software using historical claims data to predict future utilization/cost of care
Electronic/robotic patient care assistants	Cost effectiveness analytic software
Templating software tools for digital image surgical planning	Electronic guideline distribution Disease registries

EHRs, electronic health records; IT, information technology.

Furthermore, it is difficult to determine when a product is in final form, and balance the risk that arises from installation and implementation issues with that inherent at the product inception. For example, the 'build' and configuration of an EHR was considered complex and assigned a 'higher risk' (eg, a greater number of people exposed and number of processes involved) compared to that of a closed-loop insulin pump with an implanted continuous glucose monitor, which was assigned a 'medium risk.' Automated decision-making, which is synonymous with intelligent IV pumps, was also considered complex and assigned a 'higher risk' compared to an mHealth nutrition app, which provided information only and was assigned a 'lower risk.'

WHAT CURRENT REGULATORY FRAMEWORKS ARE IN PLACE?

The Center for Devices and Radiological Health of the FDA is responsible for assuring the safety, effectiveness, and proper labeling of medical devices and radiation-emitting products marketed in the USA. A product will be regulated as a medical device if it meets the definition set out in the Federal Food, Drug, and Cosmetic Act (see box 1). A medical device can be assigned to one of three classes, that is, class I, II, or III, depending on its intended use and its indications for use.[2] Regulatory control increases from class I to class III. For example, approximately 74% of class I devices (which pose a low risk of illness or injury) are exempt from the premarket notification process,[2] whereas most class III devices (which are considered to pose a greater risk) require premarket approval. Although the FDA's regulatory requirements can help ensure the safety and effectiveness of medical devices, the FDASIA working group highlighted

Table 2 Framework for risk and innovation dimensions of assessing risk by patient harm[3]

	Lower risk	Medium risk	Higher risk/more attention
Purpose of software product	Information only; purpose is transparent and clear	Makes recommendations to user	Automated decision making (eg, intelligent intravenous pump, automated external defibrillator)
Intended user(s)	Targeted user(s) are knowledgeable and can safely use product	Makes recommendations to knowledgeable user	Provides diagnosis or treatment advice directly to knowledgeable user
Severity of injury	Very low probability of harm	Potential for non-life threatening adverse event	Life-threatening potential
Likelihood of hazardous situation arising	Rare (<1 per 10 000 patient-years)	Unpredictable, but hazardous situation arises >1 per 10 000 patient-years and less than once a year	Common (arises once per year)
Transparency of software operations, data, and included content providers	Software output is easy to understand and its 'calculation' (data and algorithm) transparent	Software operates transparently and output is understandable by software expert	'Black box'
Ability to mitigate harmful conditions	Human intermediary knowledgeable and empowered to intervene to prevent harm	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	Application of mature, widely adopted technologies with information output that is easy to understand by the user	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product	Complexity of data collection and 'transformation' involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	The 'build' and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily	The 'build' and configuration of the software is moderately complex, but 'guard rails' significantly limit types of changes that might induce life-threatening risk	The 'build' and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no 'guard rails'
Complexity of training and use	The software system output is clear and easy to interpret. Minimal training is needed	Moderate complexity. Less than 2 h of training required	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary
Use as part of more comprehensive software/ hardware system	Used as a standalone product, or output is unambiguously used as part of a larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	Software interacts with 1–3 other systems with mature, well-described interfaces	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm (eg, DDI thresholds)
Network connectivity, standards, security	Wired and wireless licensed spectrum	Wireless spectrum that is licensed by rule with interference protection and low risk of harmful interference	Wireless unlicensed spectrum, which has no protection from harmful interference

DDI, drug drug interaction.

Box 1 Definition of a medical device

A device is:
an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- 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 any of its primary intended purposes.[8]

how such regulations were geared especially, but not exclusively, to physical devices. It was felt that this could stifle the pace and diffusion of innovation, or otherwise discourage manufacturers from introducing new software to the market. The group therefore suggested that health IT should not be subject to FDA premarket notification, except for: (i) medical device accessories, (ii) certain forms of high risk clinical decision support, such as computer-aided diagnostics, and (iii) higher risk software, where the intended use elevates the aggregated risk. The group also recommended that the FDA define the scope of regulations for each of the suggested exemptions listed above. A robust postmarket surveillance mechanism, with post-implementation testing to track adverse events and near misses, was also recommended.

The ONC Certification Program set the standards, implementation specifications, and certification criteria that EHRs must meet, at a minimum, to support the achievement of meaningful use.[4] To qualify for the financial incentives offered under the Medicare and Medicaid EHR Incentive Programs,[5] healthcare professionals and hospitals must both adopt certified EHRs and demonstrate meaningful use of this technology. A number of organizations are involved in testing and certifying EHR products, including the accredited testing laboratories and authorized certification bodies, respectively. The FDASIA working group commented on how certifying specific test behaviors can limit innovation, favoring existing software with defined 'best practice' features. The group suggested providing more flexibility around compliance to accommodate new health IT developments, and greater transparency and predictability of candidate standards that are being considered for possible adoption. It was also recommended that the ONC, FDA, and FCC should avoid any regulatory duplication, as it is possible for the same medical device to be brought independently before all agencies.

ARE THERE BETTER WAYS TO ASSURE THAT INNOVATION IS PERMITTED TO BLOOM, LOCAL AND NATIONAL ACCOUNTABILITY ENCOURAGED, AND SAFETY PROMOTED?

The FDASIA working group was clear that any new regulatory framework for health IT should promote innovation. Transparency of products and results was proposed as one way in which innovation could be stimulated. The availability of comparative information about a particular product, for example, could drive choice and help healthcare organizations improve their performance. The working group highlighted how national standards for quality processes should also be measurable and transparent. Standards and specifications that support interoperability could help bring more proposed solutions to market; industry participation in the development of such standards was encouraged. The working group also recommended more local health IT configuration and integration, as well as more control and accountability for outcomes of use. This included the ability to iteratively develop, design, test, and implement changes to meet users' needs. Furthermore, the Institute of Medicine (IOM) report *Health IT and Patient Safety: Building Safer Systems for Better Care* recommended the reporting of health IT-related adverse events by vendors and users to identify and rectify vulnerabilities that threaten safety.[6] This was echoed by the working group, who emphasized the importance of non-punitive reporting of safety issues and the aggregation of these data at a national level to help drive outcome improvements.

More research is needed to explore the root cause of health IT system-related errors, and the huge challenges that surround the secure exchange of confidential clinical information among disparate systems and healthcare settings. Addressing key gaps in EHR functionality is essential for all healthcare providers, and broader access to safety and system performance data is needed to facilitate timely improvements. In response to this Health and Human Services report, the health informatics community may be encouraged to develop and adopt best practices in the safe design, deployment, and use of EHRs, as well as share information about obstacles encountered during health IT implementations. Although much has been accomplished to date, considerable additional progress is needed to track adverse events and near misses for certain health IT functionality, and create a healthcare environment where patient safety is protected. Health IT developers and vendors may also be required to list products that represent at least some risk and encouraged to report serious health IT-related safety events. The working group viewed the sharing of information, knowledge, and lessons learned as fundamental to promoting safety and innovation.

FUTURE DIRECTIONS

The next step will be for Health and Human Services to release its report for public commentary. This report is of great significance to the health informatics community as it paves the way for possible risk-based regulation of health IT in the coming years and for reducing barriers to innovation. The health IT industry also has a great deal of interest in the recommendations. Too much regulation could stifle innovation, while if little oversight is put in place, safety issues may remain uncorrected.[6] While health IT is likely highly beneficial in the aggregate with respect to safety, numerous unintended consequences of health IT have been identified,[7] and it does not necessarily result in desired benefits.

It remains to be seen which, if any, of the recommendations the federal agencies will take on board and the likely impact such a report will have on the future health IT agenda. We await the next developments with interest.

Contributors SPS and DWB conceived and wrote this article. They both act as guarantors.

Competing interests DWB served as chair of the FDASIA Workgroup, and is a member of the HIT Policy Committee.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1 Food and Drug Administration Safety and Innovation Act of 2012.
2 U.S. Department of Health & Human Services. *Food and Drug Administration*. http://www.fda.gov/ (accessed 28 Mar 2014).
3 Office of the National Coordinator for Health Information Technology (ONC) website. *Draft FSASIA Committee Report*. http://www.healthit.gov/FACAS/calendar/2013/08/13/policy-fdasia (accessed 28 Mar 2014).
4 Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services. *Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Record Technology*. *Final Rule*. 45 CFR Part 170. 2010.
5 Centers for Medicare & Medicaid Services. *Medicare and Medicaid Programs; Electronic Health Record Incentive Program*. *Final Rule*. 2010.
6 IOM (Institute of Medicine). *Health IT and patient safety: building safer systems for better care*. Washington, DC: The National Academics Press, 2012.
7 Ash JS, Berg M, Coiera E. Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *J Am Med Inform Assn* 2004;11:104–12.
8 Federal Food, Drug & Cosmetic Act of 1938, US 52 Stat. 1040.