

June 28, 2013

Jodi Daniel  
Director, Office of Policy and Planning  
Office of the National Coordinator for Health Information Technology  
U.S. Department of Health and Human Services  
200 Independence Avenue S.W.  
Washington, D.C. 20201

**RE: Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology**

Dear Ms. Daniel:

On behalf of McKesson Corporation (“McKesson”), I am pleased to submit comments to the Office of the National Coordinator for Health Information Technology (“ONC”) on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology. We commend the ONC for its efforts to ensure patient safety through appropriate oversight, and we applaud ongoing initiatives to support innovation and promote the broad adoption of health information technology (health IT).

For 180 years, McKesson has led the industry in the delivery of medicines and healthcare products. As the largest health IT company in the world, we are actively engaged in the transformation of healthcare from a system burdened by paper to one empowered by interoperable electronic solutions that improve patient safety, reduce the cost and variability of care and advance healthcare efficiency. McKesson has decades of experience serving the health IT needs of the largest and most diverse provider base in the industry, including 50 percent of all health systems, 77 percent of health systems with more than 200 beds, 20 percent of all physician practices and 25 percent of home care agencies, which support more than 50,000 home care visits annually. We process billions of financial healthcare transactions annually among physicians, hospitals, pharmacies, insurers and financial institutions, and provide care and claims management solutions to most of America’s health insurance companies. We also manage millions of aggregated personal health records, connecting patients online with their physicians, hospitals, reference laboratories and health plans.

McKesson has a long history of leadership and collaboration with the industry in the area of patient safety. Our perspective on the regulation of health IT is based on our extensive experience and informed by our belief in the power of health IT to improve the quality, safety and efficiency of healthcare. We appreciate the opportunity to share our point of view.

**Executive Summary**

Health IT is foundational to improving the quality, safety and affordability of healthcare and to the successful implementation of healthcare reforms. McKesson supports a regulatory approach to health IT that promotes quality, assures patient safety and fosters innovation.

**In order to leverage the power of those solutions to transform healthcare, a new regulatory framework must be created that is *specific* to health IT.**

Three key factors should guide the development of a new framework for health IT:

**1. Regulation of health IT should be risk-based.**

Health IT should not be subject to a one-size-fits-all regulatory framework. Instead, oversight should increase or decrease in proportion to the relative risk to patient safety. That risk is best defined as the severity of the harm to a patient and its likelihood of occurrence. The likelihood of harm depends upon whether the technology directly acts on the patient or whether it merely aggregates data and informs or advises a clinician.

**2. Not all health IT should be regulated as “medical devices”.**

The current regulatory approach for medical devices is not appropriate for health IT. The Food and Drug Administration (FDA) medical device laws and regulations drafted decades ago did not envisage the technological advances in modern healthcare and are not well suited to rapidly changing and dynamic technology. Moreover, there are fundamental differences between medical devices and health IT. Most medical devices are directly used in the diagnosis or treatment of a patient, with little if any opportunity for the clinician to intervene. However, the majority of medical software, including clinical decision support and electronic health records (EHRs), does not directly diagnose or treat the patient, but rather provides data and guidance to clinicians in their assessment or treatment of a patient. The ability of the physician to utilize professional judgment when interacting with these forms of health IT makes these types of technology fundamentally different from traditional medical devices.

**3. Regulation of health IT should not automatically default to FDA.**

The safety of most medical devices is almost entirely dependent on how the devices are designed and manufactured. In contrast, the safety of health IT systems is dependent on how they are customized, implemented and used as well as designed. The FDA does not have the expertise to provide oversight of implementation and use of technology; it also lacks the statutory authority to regulate physicians, nurses, hospitals and other providers who implement, customize and use health IT. While the FDA should retain jurisdiction over certain types of health IT, as discussed below, many other types of health IT would be more appropriately and effectively governed by a new regulatory framework outside of the FDA.

With these factors in mind, we offer our recommendations for a new risk-based regulatory framework and respond to the specific questions posed by the ONC.

**A New Framework for Health IT**

Under the auspices of the Bipartisan Policy Center (BPC), McKesson in concert with hospital, physician and patient organizations, and other health IT companies has developed consensus recommendations for a new risk-based framework for health IT. These recommendations are outlined in the BPC Report: [An Oversight Framework for Assuring Patient Safety in Health Information Technology](#) and were developed to advise the FDA, ONC and the Federal Communications Commission (FCC) as they respond to the congressional requirement to develop a new risk-based regulatory framework specific to health IT.

The BPC’s recommendations divide health IT into three categories according to the relative risk to patients and the opportunity for clinical intervention.

- **Medical device software** often directly interacts with the patient or another medical device with little or no opportunity for clinical intervention. This class of health IT represents a higher potential risk of patient harm. Such devices are currently regulated by the FDA as Class I, Class II, or Class III medical devices.

As indicated above, we recommend no change in how medical device software is regulated. Continued FDA regulation of these kinds of technology is appropriate.

- **Administrative software** supports the administrative and operational aspects of healthcare but is not used in direct delivery of clinical care. Population analytics, back office billing systems, claims payment systems, and prescription drug refill reminders are all examples of software that is not used for patient specific treatment or diagnosis. This class of health IT represents the lowest level of risk of patient harm. Accordingly, we recommend no additional oversight.
- **Clinical software** captures, analyzes or presents patient specific or population-based data which can be used to recommend a course of care. This class of health IT represents a low to moderate risk of patient harm.

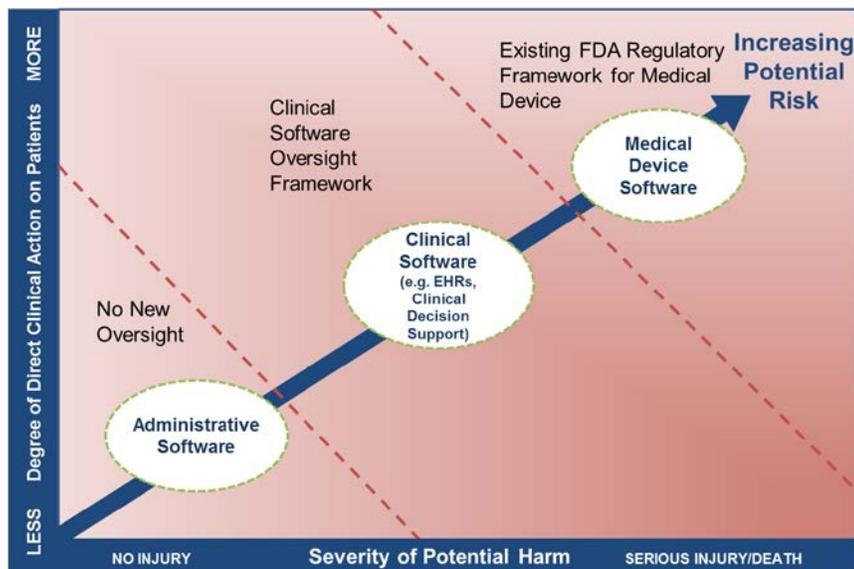
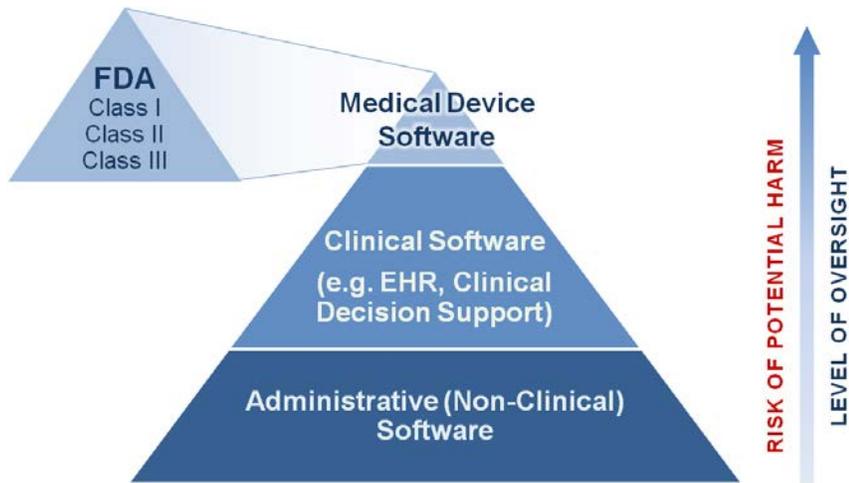
Clinical software is the category that requires a specific and new framework. Regulation of this category of software should reflect the shared responsibility for patient safety among health IT developers, those responsible for implementing and customizing the systems, and, ultimately, the end user in a clinical setting. As such, the framework should include oversight of both the development and deployment of the software.

- a. Development: Clinical software such as decision support, EHRs and related software are a unique form of technology and should therefore be regulated by an organization with proven capabilities in the fields of technology, clinical care delivery and healthcare practice. Organizations such as the National Committee for Quality Assurance (NCQA) or URAC have track records in the rigorous accreditation of healthcare software.
- b. Implementation, customization and use: Provider oversight of software deployment should mirror similar processes and procedures involving patient safety, such as infection control and medication safety. Organizations such as The Joint Commission are well suited to rigorous accreditation of practices governing patient-facing delivery of care.

Organizations such as The Joint Commission, NCQA and URAC have the expertise to evaluate and accredit developers, providers and users of health IT. The ONC is well positioned to coordinate oversight among these various organizations to ensure patient safety, prevent overlap and continue to foster innovation and adoption of health IT by providers.

Establishing clear classes of health IT, subject to varying oversight by those best positioned and with the most applicable expertise, will result in a regulatory pathway that ensures patient safety, fosters innovation and encourages broad and timely adoption of health IT.

The charts below depict our vision of the new regulatory framework.



**Responses to Specific Questions Posed by the ONC**

Below are McKesson’s specific responses to questions posed by the ONC.

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

As indicated above, we endorse BPC’s recommendation that health IT be considered in three classes, according to the relative risk to patients. We recommend that the report include all three classes: medical device software, clinical software and administrative software. The FDA should retain authority over medical device software, the ONC should be responsible for coordinating standards and accreditation of clinical software, and no additional regulatory oversight should be required for administrative software.

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

As Dr. Farzad Mostashari said during his remarks at a February 2013 BPC event, “health IT is part of the patient safety solution.” Health IT provides access to current accurate patient information such as medical history. It supports the clinician in preventing errors, identifying gaps in care and suggesting appropriate diagnostic and treatment paths.

Health IT does not replace physician judgment, but rather provides guidance and support. The ultimate responsibility for a patient will always rest with the treating clinician. As with any type of technology, a certain degree of risk may be introduced into the system; however, this risk varies widely depending on the context of the use of the software. Consequently, the BPC recommended a framework which is predicated upon two key components of risk: the severity of patient harm that could result from the use of the software, and the opportunity for clinical intervention.

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

In addition to the points raised above, we recommend consideration of the following in the development of a new regulatory approach for health IT:

- ***Use of Existing Standards***  
McKesson encourages the agencies to draw upon the extensive body of international standards that have been established by Standards Development Organizations, primarily under ISO, which are focused specifically on health IT. These standards address the unique software development life cycle.
- ***Configuration and Use of Health IT***  
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.
- ***Expertise***  
A new framework should vest oversight authority with those possessing the expertise necessary to evaluate health IT and should use the risk analysis suggested above. The FDA’s expertise is in regulating devices through oversight of manufacturing, production and quality control processes. Oversight of health IT requires expertise in the customization, implementation and use of software across multiple healthcare systems and settings. More importantly, the lengthy FDA approval process is not designed to respond to the rapidly evolving life cycles of software development.
- ***Innovation***  
The oversight framework for safety in health IT should promote, not stifle, the innovation needed to drive advances in healthcare. Health IT plays a critical role in improving the quality, safety and cost-effectiveness of care and is essential to the successful implementation of healthcare reforms. Current regulatory frameworks which are oriented towards manufactured devices that change infrequently and are not typically customized to the needs of the user will neither effectively support nor promote the current and anticipated rapid development of health IT.

- ***Collaboration***  
Any oversight framework for safety in health IT should have strong support from and the involvement of all stakeholders: patients, health IT developers, implementers and users. Such collaboration is already underway among industry stakeholder groups such as that formed under the auspices of the BPC.
- ***Platform Neutrality***  
An appropriate regulatory approach for health IT should be specific to the technology use and based on potential patient safety risk; the platform on which the software is deployed should not determine its regulatory framework. Mobile or cloud-based applications should not be regulated differently from traditional server-based systems unless the platform substantially impacts the relative risk of the technology.

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

Many organizations are actively involved today in patient safety initiatives, including the FDA, FCC, the Agency for Healthcare Research and Quality (AHRQ), state programs, Patient Safety Organizations (PSOs), ONC-ACBs, the National Institute of Standards and Technology (NIST), the National Library of Medicine (NLM) and the Center for Medicare and Medicaid Innovation (CMMI). The ONC has stated that it will function as a “convener.”

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.

Traditionally, the FDA has regulated the software imbedded in medical devices, such as the applications which run pacemakers and diagnostic equipment. The agency also regulates stand alone software that closely integrates with these devices, such as picture archiving systems (PACS) and laboratory information systems (LIS). Recently, FDA initiated rulemaking activities for mobile medical applications and is now considering regulation of decision support software and electronic medical records.

Finally, the FCC recently announced the appointment of a Director of Health Initiatives charged with leading “the agency’s efforts in facilitating and promoting communications technologies and services that improve the quality of health care for all citizens and help reduce health care costs.” This begs the question as to who will ultimately have jurisdiction over health IT and the electronic transmission of health information.

Jurisdiction among multiple agencies creates potential overlap as well as ongoing uncertainty. Examples are as follows:

In the draft FDA Mobile Medical Applications guidance, FDA states that “although some mobile apps that do not meet the definition of a mobile medical app may meet the FD&C Act’s definition of a device, FDA intends to exercise enforcement discretion towards those mobile apps.” FDA “strongly recommends that manufacturers of all mobile apps that may meet the definition of a device follow the Quality Systems regulations, which include good manufacturing practices, in the design and development of their mobile medical apps.”

At the same time, ONC may be considering a requirement for a Quality Management System (QMS) as part of EHR certification or the ONC patient safety surveillance plan. This type of uncoordinated guidance and rulemaking could result in an overlap with FDA's QMS requirements that will cause significant confusion.

**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?**

We believe the ONC is well positioned to oversee and promote health IT safety. We also believe that 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.

As the ONC collaborates with the FDA and FCC to consider the development and implementation of a risk-based regulatory framework for health IT, we strongly recommend that you also draw upon the expertise of other groups engaged in similar processes, such as the BPC.

**Conclusion**

McKesson appreciates the opportunity to provide comments to the ONC and to share our perspective on the development of a risk-based regulatory framework and strategy for health information technology. Health IT is imperative to the successful transformation of healthcare. It improves quality and patient safety, enables payment and delivery reform and promotes efficiency and lower costs.

We offer the following recommendations in support of the successful development and implementation of a new, risk-based regulatory framework *specific* to health IT:

- Establish categories of health IT based on relative risk to patients and the opportunity for clinical intervention;
- Leverage existing international standards that have been established by Standards Development Organizations, primarily under ISO, that are specific to health IT;
- Adopt platform neutrality as a characteristic of the framework;
- Utilize organizations such as The Joint Commission, NCQA and URAC which have the expertise to evaluate and accredit developers, providers and users of health IT; and
- Develop a process for coordinating the oversight of health IT across all federal agencies.

It is essential that the ONC coordinate with all relevant agencies and stakeholders to ensure that authority and accountability are aligned and synergies are created. McKesson is prepared to support the Administration as you develop a coordinated, streamlined process for ensuring patient safety and promoting innovation in the broad adoption of health IT.

We appreciate the opportunity to provide our recommendations. Should you have questions or need further information, please contact me at (415) 983-8494 or [ann.berkey@mckesson.com](mailto:ann.berkey@mckesson.com)

Sincerely,



Ann Richardson Berkey