33 W. Monroe Street, Suite 1700
Chicago, IL 60603-5616

Tel 312 664 4467
Fax 312 664 6143

www.himss.org

July 17, 2013

Dr. Farzad Mostashari, M.D., ScM
National Coordinator
Office of the National Coordinator for Health IT
U.S. Department of Health and Human Services
Washington, DC 20201

Dear Dr. Mostashari:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to offer written comments requested by the Food and Drug Administration Safety and Innovation Action (FDASIA) Workgroup, in response to its Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology.

HIMSS is a cause-based, not-for-profit organization focused on better health through information technology (IT). Globally, HIMSS leads efforts to optimize health engagements and care outcomes using information technology. HIMSS is a part of HIMSS WorldWide, a cause-based, global enterprise producing health IT thought leadership, education, events, market research and media services around the world. Founded in 1961, HIMSS WorldWide encompasses more than 52,000 individuals, of which more than two-thirds work in healthcare provider, governmental and not-for-profit organizations across the globe, plus over 600 corporations and 250 not-for-profit partner organizations, that share this cause.

Further, in recognizing the growing role of mobile and wireless devices in health and healthcare, HIMSS created mHIMSS in 2011 to focus on the use of mobile and wireless technologies to promote health, improve the quality, accessibility and safety of care, and increase the cost-effectiveness of care. mHIMSS builds on the existing HIMSS strengths of convening stakeholders, sharing knowledge, providing world-class education, public policy, research, and content – entirely focused on the use of mobile technologies.

The Request for Comments seeks input in three categories areas; our comments are divided into those respective categories below.

Taxonomy

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

Section 3000(5) of the HITECH Act defines the term "health information technology" as hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."[1] HIMSS suggests that when conducting an analysis of health IT regulation, the agencies and workgroup should take a broad approach and consider the full range of health information technology products and software. To that

[1]Public Law 111-5; February 2009: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

end, HIMSS notes that health IT applications are used as part of a rapidly evolving system of systems with shared responsibility among multiple stakeholders.

In general, HIMSS recommends encouraging innovation, and avoiding burdensome regulatory structures. HIMSS has historically counseled against an FDA definition of "medical device" that includes software or hardware if it is not integral to the functioning of a traditional diagnostic, therapeutic, or surgical device[2], and that the definition of "medical device" should not cover software or hardware that provides clinical decision support, an Electronic Health Record (EHR), simply transmits or allows other parties to read information originally sent from a medical device, or is a technology widely used in other industries. We reiterate this recommendation to the FDASIA workgroup.

Risk Assessment & Innovation

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

HIMSS strongly emphasizes that health IT is an effective enabler of safety and provides the tools necessary to facilitate broader patient safety reporting. However, there are potential risks for health IT as it is used in practice and the potential for unintended consequences (e-iatrogenesis). Such risks, which can arise from development, implementation deployment, or use of health IT, can include: increased or new work, extended workflow, system demands, communication, new kinds of errors and potential dependency on the system. Therefore, post-market risks beyond the classification of a particular product, like to actual usage and usability of technology, should be acknowledged. Ample training and continual follow-up on workflow by both vendors and users should be integrated with technology implementation.

Health IT systems must be safe and be designed in a usable way to optimize user workflow. Processes need to be efficient so as to enable "meaningful users" and accountability for providers in their roles and in their contribution to patient care. Technology-enabled delivery systems should contribute to a broader "Learning Health System" in which the culture is team-based, patients and the public are engaged, and a trust fabric is strong, protected and actively nurtured.

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

In HIMSS' System Risk Analysis Survey, we found that medical technology has rapidly evolved in the past 20 years and does not resemble last generation technology, which guided many of the guidelines and regulations that are still in effect today. New technologies also bring new challenges and vulnerabilities. We strongly support the application of effective risk management to information technology and associated processes by healthcare providers as absolutely critical to addressing the challenges associated with these increasingly complex and integrated technologies. Application of effective risk management can identify major technology-related risks and enable organizations to focus finite resources on priority issues and realize tangible benefits.

HIMSS notes that the discussion of potential regulation of certain types of health IT should fully reflect the complexity of health information systems as part of a diverse system of care delivery. It is our view that health IT plays a significant role in increasing patient safety, but we also recognize that health IT is

[2]HIMSS Statement for the Record to the House Energy and Commerce Committee; March 23, 2013: http://www.himss.org/files/HIMSSorg/Content/files/HIMSS_statement_record_EC_TechnologySubcmte.pdf

a part of a system of information, and problems with software or technology has the potential to add to safety problems. We note that any regulatory scheme that focuses only on one element of a social and technical system issue may lack a holistic approach to enhanced patient safety.

For the FDASIA Workgroup, we suggest that an appropriate, risk-based regulatory framework should use the following factors to first assess risk and then to determine the level of oversight or regulation to apply to a health IT product or category of products.

- Identify potential harms in the event of a product failure, delivery latency (criticality dependent), or incorrect data;
- Stratify by the purpose of the IT product or category as it relates to a patient's health;
- Consider the impact to existing efficiency, effectiveness, accountability and liability prior to instituting new or expanded regulation;
- Consider the level of reliance on the health IT product by patients and healthcare providers and balance the benefits of the product or category to improve health care delivery with the costs of regulation or new programs on innovation;
- Determine potential harm mitigation including clinician or patient interventions, safety features/controls and oversight, and determine risk assessment steps,
    - Catalog the severity, likelihood and potential outcome of each potential harm;
    - Ascertain if risk is preventable, and whether periodic internal or external technical checks might improve quality control
    - If mitigation is possible, determine whether the risk can be assessed and corrected by a single party or whether it requires an assessment by, and the efforts of, multiple parties.

Finally, in considering a framework, HIMSS encourages efforts leading toward a nationwide patient data matching strategy, including: the prevalence and costs of patient-data mismatches and subsequent corrections nationwide, the patient safety risks of not having a nationwide strategy, the benefits and implications of applying a nationwide strategy, the impact on privacy, security, and safety of a nationwide strategy, current and near-term available technologies, the costs/benefits and practicality of adopting a nationwide strategy, and best industry practices currently employed to ensure acceptably reliable patient data matching across systems while enhancing patient privacy, security, and safety.

Regulation of Mobile Technologies

As a general note, in considering regulation on mobile technology specifically, HIMSS Policy Principles state and endorse the following points related to regulation and mobile health technologies.

13.1 Promote clinical and financial effectiveness, as well as efficiency associated with the use of mobile health technologies (mHealth).

13.2 Integrate mobile technologies into the design and deployment of healthcare information technology systems to leverage current and future incentives associated with ONC's Meaningful Use definition and CMS's Incentive Payments regulations.

13.7 Encourage and promote the coordination and simplification of mobile-focused standards of operation and data protocols by engaging with existing and emerging bodies governing the certification of mobile apps and other processes.

13.9 Encourage collaboration with private sector innovators developing medical apps for use in mobile healthcare settings.

13.11 Collaborate with stakeholders to work towards a unified regulatory approach in the field of mHealth.

HIMSS appreciates this opportunity to provide public comment for this current phase of the FDASIA Workgroup's efforts. We look forward to continuing the dialogue with the Workgroup and the Department on this complex topic. For more information, please contact Thomas M. Leary, Vice President of Government Relations, 703.562.8814 or Stephanie Jamison, Director of Government Services, 703.562.8844.

Sincerely,

Scott T. MacLean, MBA, CPHIMS, FHIMSS
Chair, HIMSS Board of Directors
Deputy CIO, Director of IS Operations
Partners HealthCare in Boston, MA

H. Stephen Lieber, CAE
President/CEO

CC:
Jodi Daniel, JD, Director, ONC Office of Policy and Planning
Steve Posnack, MA, Director, ONC Office of Policy and Planning, Federal Policy Division