



TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org

Tel: +1.703.907.7700
Fax: +1.703.907.7727

Submitted via www.regulations.gov

August 31, 2013

**Steven Posnack
Director
Federal Policy Division, Office of Policy and Planning
Office of the National Coordinator for Health IT**

Re: *Answers to Questions Posed in 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 [HHS-OS-2013-0003-0001]*

I. Introduction, Statement of Interest, and General Views

The Telecommunications Industry Association (“TIA”) hereby submits comments on the Office of the National Coordinator for Health Information Technology, Department of Health and Human Services (“ONC”) request for input to inform the development of a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework for health IT, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication.¹

¹ Food and Drug Administration Safety and Innovation Act: Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology, 78 Fed. Reg. 32390 (May 30, 2013).

TIA is a trade association representing approximately 500 participating companies, which are manufacturers and vendors of health information technology (“health IT”).² TIA provides an advocacy voice in Congress, across Federal agencies, and, internationally, on numerous industry priority issues including health IT. TIA is also a standards development organization since its inception in 1988, and is one of the largest standard development organizations (“SDOs”) accredited by the American National Standards Institute (“ANSI”). TIA’s standards committees create consensus-based voluntary standards for numerous facets of the health IT industry. Such standards are utilized by both private sector interests and government, which are directly affected by the policies of the U.S. Government in the sweeping area of health information technology. Among other areas, TIA’s standards committees develop protocols and interface standards relating to current U.S. Government technology priorities in such areas as fiber optics, public and private interworking, telecommunications cable infrastructure, wireless and mobile communications, multimedia and voice over internet protocol (VoIP) access. TIA’s standards reach into areas such as Smart Grid, emergency communications infrastructure, and – of particular relevance here – Health IT and machine-to-machine (M2M). TIA’s member companies³ provide, develop, manufacture, and supply health IT products and services. The services include electronic health record (“EHR”) systems that qualify for Medicare and Medicaid EHR incentive payments under the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.⁴ TIA members occupy critical roles in the mHealth community, producing many of the mobile products, medical devices and applications which have become increasingly powerful tools for innovative health care solutions. TIA members are part of the overwhelming consensus of stakeholders who believe that medical devices, enabled by high-speed wireless communications, hold great potential to help medical professionals

² 42 USCS § 300jj(4) defines health IT 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.”

³ For a list of TIA members, see <https://www.tiaonline.org/about/member-list>.

⁴ Pub. L. No. 111-5 (2009), at § 13000 *et seq.*

more quickly and efficiently support patients, while also providing consumers with better access to health information and tools in a secure manner. We also recognize that the safety of patients is a shared responsibility that cuts across a diverse group of stakeholders, including the care provider, the appropriate regulator, product innovators and developers, and patients, among others.

Generally, TIA believes that the report for Congress generated pursuant to this input should emphasize that over-regulation in the innovative and dynamic field of health IT is a disincentive to investment, ultimately stifling innovation and harming the American patient. Initially, TIA wishes to express its strong belief that no further regulatory burdens be added to existing regulations in the health IT space. The future of health IT regulation should focus on enhancing opportunities and avoiding requirements which will prevent the development of better services and products. Moving forward, the regulatory and oversight landscape should remove duplicative and unnecessary elements, and should evolve with the industry, appropriately balancing potential risk between patient harm and encouraging market entrance and innovation.

Specifically, TIA believes that the recommendation by the FDASIA Working Group should first support existing regulatory mechanisms that enable innovation while protecting patient safety and avoiding regulatory duplication. The FDASIA Working Group has so far identified several program mechanisms that would provide immediate clarity and predictability to processes by FDA, ONC and FCC.⁵ Those mechanisms should be exploited to their fullest potential to help speed innovation in health IT. Secondary, should be any recommendation for the creation of new frameworks that may be helpful but take longer to implement.

⁵ See <http://www.healthit.gov/sites/default/files/fdasiarecommendationsdraft080613.pdf>.

II. Responses to Specific Questions

1. Taxonomy

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

Food and Drug Administration (FDA)

In the report developed jointly by these agencies, FDA should address aspects of health IT including:

- Those that currently fall squarely outside the authority to evaluate (i.e. what properly constitutes a “device” under section 201(h) of the Food, Drug and Cosmetic Act (“FD&C”)),⁶ based on, among other sources of stakeholder input, consultative input from cooperating agencies such as ONC. There remains a need for the FDA to clarify and differentiate between health, wellness and the characteristics of disease-related medical claims and exempt those products that do not present a clear threat to patient safety. In particular, the FDA should utilize appropriate opportunities (e.g., when claims about a general health or wellness application could impinge status as a mobile medical application and considered a “medical device”) to establish a policy of “enforcement discretion for *lowest-risk* health IT. In addition, FDA should provide an exemption from Good Manufacturing Practices (“GMP”)⁷ for *lower-risk* health IT.
- What constitutes an accessory to a medical device. Under current rules, FDA treats anything intended to be used as an accessory to a medical device, as a medical device in its own right and regulated at the same classification level as the parent device. In health IT, in particular software that are low-risk and should not be obligated to undertake the regulatory burden of a higher classification medical device.

⁶ 21 U.S.C. §301 *et seq.*

⁷ See Good Manufacturing Practices in 21 CFR Part 820 (“GMP”).

- FDA should clarify the scope of clinical decision support software that FDA regulates, and this should include the solicitation and consideration of public input. FDA has long regulated certain forms of clinical decision support (“CDS”) software, such as CDS software that provides radiation treatment recommendation from combines multiple physiological inputs. But there are many examples of low risk CDS software that should not be regulated. FDA should work in consultation with ONC to define those CDS software products that do not present a threat to patient safety
- Software modularization exists between individual medical software and non-medical generic software modules. FDA must clarify how medical and non-medical software modules can be used jointly on the same platform. FDA should recognize the difference between medical software and non-medical software running on the same platform and address the two distinct products separately. The medical device software should not impact the non-medical software and further change its designation.
- The FDA should address the definition of “medical device” security- or cybersecurity-related issues in the following issuances and others, ensuring that they are coordinated with other agency efforts noted in this document, and, where possible, defer to existing open, voluntary, and consensus-based standards when addressing the security of devices⁸:
 - The FDA has already issued a medical device safety recommendation titled *FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks*,⁹ with steps to “assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.”

⁸ This policy would be consistent with long-standing federal policy. *See, e.g.*, OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (rev. Feb. 10, 1998) (OMB Circular A-119) *available at* <http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html>.

⁹ *See* <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm>.

- The FDA has issued draft guidance titled *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*,¹⁰ intended to “assist industry by identifying issues related to cybersecurity that manufacturers should consider in preparing premarket submissions for medical devices.”
- Increasing outreach and education efforts to stakeholders and the public. The FDA should work to improve outreach and education to affected parties and the general public about its existing and planned policies to understand the reach and effect of the same.

Department of Health and Human Services Office of the National Coordinator for Health IT (ONC)

In the report developed jointly by these agencies, ONC should address the following aspects of health IT:

- A proposed strategy and recommendations for a regulatory framework that contemplates the implementation of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.¹¹ FDASIA’s recommendations should not ignore but rather reflect the Congressional HITECH Act’s aim to promote and expand the adoption of health information technology by creating a nationwide network of electronic health records. While ONC current focus has been on increasing the use of EHR systems under HITECH, EHRs are but one key component of the larger effort to improve the American healthcare system. ONC should now address its proposed strategy and recommendations on standards and certification of interoperable medical devices and the ability to upload patient generated health data (PGHD) into certified EHR and EHR Systems.

¹⁰ See <http://www.gpo.gov/fdsys/pkg/FR-2013-06-14/pdf/2013-14167.pdf>.

¹¹ Pub. L. No. 111-5 (2009), at § 13000 *et seq.* (“HITECH Act”).

- In this way ONC is a key driver of health IT interoperability and should include medical device and PGHD into its framework for Meaningful Use Stage 3 and future stages.
- ONC should play a major role in helping to define which low-risk software falls outside of FDA regulation and is currently regulated through existing standards, certification, and through safety and security standards articulated by NIST.

Federal Communications Commission (FCC)

In the report developed jointly by these agencies, the FCC should address the following aspects of health IT:

- Universal service-related:
 - The FCC's Healthcare Connect Fund, capped at \$400m, created to expand health care provider access, or "telehealth," to broadband, especially in rural areas, and encourage the creation of state and regional broadband health care networks. The fund provides a 65% discount on broadband services, equipment, connections to research and education networks, health care provider-constructed and owned facilities if shown to be the most cost-effective option.¹² Referring to the National Broadband Plan, the FCC defines "telehealth" as "the broad range of health care-related applications that depend upon broadband connectivity, including telemedicine; exchange of electronic health records; collection of data through Health Information Exchanges and other entities; exchange of large image files (e.g. X-ray, MRIs, and CAT scans); and the use of real-time and delayed video conferencing for a wide range of telemedicine, consultation, training, and other health care purposes."¹³ This important program's goals and activities should be considered, and the FCC and others

¹² See *Rural Health Care Support Mechanism*, WC Docket No. 02-60, Report and Order, 27 FCC Rcd 16678 (2012).

¹³ See *Id.* at FN 49.

should look to proactively prevent duplicative or conflicting requirements, and to augment and coordinate policy goals.

- Radio frequency-related (spectrum management/specific allocations):
 - There is a need for continued, cross-agency coordinated, inquiries into opportunities for mobile broadband allocations that can be utilized by healthcare applications. These include both exclusive-licensed as well as unlicensed (Parts 15 or 18).
- Security- or cybersecurity-related:
 - The FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), formed under the Federal Advisory Committee Act,¹⁴ provides recommendations to the Commission regarding best practices and actions the Commission may take to ensure the security, reliability, and interoperability of communications systems. These recommendations have informed numerous regulations adopted by the FCC. TIA is a long-time member of the CSRIC, now on its fourth two-year cycle. This important effort should be better coordinated with the FDA, ONC, and other agencies with related efforts.

2. Risk and Innovation

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

TIA urges for the recognition that increased barriers to the streamlining and systemization the healthcare system, resulting in lack of or delayed implementation, create a continued and growing risk to patient safety. These resulting risks manifest themselves through a number of symptoms including less effective, duplicative, and/or delayed treatment. In addition, delayed improvements to the healthcare system will result in gross waste of resources including

¹⁴ 5 U.S.C. App. 2.

administrative costs: for example, the Institute of Medicine, the National Academy of Science's health arm, has estimated that the U.S. health care system squanders \$750 billion a year through unneeded care, byzantine paperwork, fraud and other waste, and other means.¹⁵

We understand that with enhanced remote electronic access to data being made available, there will always be some degree of risk of harm to patient safety in the areas of data privacy and security, especially when compared to no electronic availability.¹⁶ Health IT manufacturers and vendors recognize these risks and take them seriously. These manufacturers work with their customers to ensure that security and cybersecurity risks are adequately incorporated into enterprise risk management, however, to what degree does vary on the needs of the customer. More and more, security and cybersecurity concerns are of increasing importance to health care service providers. We note that unsecured enterprise systems are a principal attack vector through which Internet service provider ("ISP") and carrier network operations are attacked because ISPs are frequently connected to unsecured enterprise systems and have widely known and exploited vulnerabilities. Furthermore, it is well-documented that a large majority of successful security and cybersecurity attacks can be prevented through efforts to increase awareness of cybersecurity issues among both institutional users and the general public through better cyber "hygiene."¹⁷ TIA strongly supports Federal efforts to increase awareness of cybersecurity issues among both institutional users and the general public.

¹⁵ See IOM, *The Healthcare Imperative: Lowering Costs and Improving Outcomes* (rel. Feb. 24, 2011), available at <http://www.iom.edu/Reports/2011/The-Healthcare-Imperative-Lowering-Costs-and-Improving-Outcomes.aspx>.

¹⁶ HHS' Office of Civil Rights ("OCR") has indicated that theft and loss (lost/stolen laptops, thumb drives, smartphones; stolen paper files; etc.) continue to be major problems and that paper records continued to be a major source of breached records. See <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>. While cybersecurity-based incidents are a significant problem and tend to capture the public's attention, covered entities should not lose their focus on the more common threats posed by theft and loss.

¹⁷ Cyber "hygiene" refers to easy-to-implement strides that health IT users can take to increase cybersecurity. Cyber "hygiene" may include: training and awareness; restructuring health IT hardware and end-user devices; installing recommended software patches; and other steps to reinforce well-known security controls.

TIA, like many others, believes that health care is a major growth area for M2M communications. Globally, we project M2M spending associated with healthcare to gross more than \$2 billion in the next two years.¹⁸ There are direct societal benefits to enhanced health IT M2M communications, such as providing hospitals with the location of critical mobile equipment and reducing the time it takes health care workers to access that equipment in an emergency.¹⁹ Studies already demonstrate that patients who log their thoughts and behaviors via mobile apps or sensors, so that doctors can monitor them between visits, receive better care overall.²⁰ Examples include how remote monitoring is utilized in home settings for the most chronically ill: monitoring of IV infusions, measuring of blood glucose levels, tracking blood pressure, heart rate, and medical grade weight scale readings from the non-hospital setting to health care workers, among many others. These and other critical information datasets can be automatically sent to medical professionals who can analyze trends and alert physicians or care providers, to identify the onset of problems quickly. Systems can also determine the location of ambulances and deploy them efficiently to reduce the time it takes to respond.²¹ All of the described benefits are effects that directly correlate with the inclusion of PGHD, particularly via mobile medical applications, in the nation's health care system.²² Based on the benefits of PGHD, TIA believes that any proposed strategy and recommendations for a regulatory framework should encourage the use of PGHD and align with Meaningful Use and the CMS Incentive Payment Program. To not incentivize these technologies has the opposite effect of denying the benefits of improved healthcare to millions of American patients, thereby reducing patient safety.

¹⁸ See TIA 2013 ICT Market Review and Forecast at 2-13.

¹⁹ See <http://www.amednews.com/article/20120813/business/308139963/7/>.

²⁰ See <http://www.informationweek.com/healthcare/patient/patient-generated-mobile-data-improves-c/240008018>.

²¹ For example, George Washington University's Heart and Vascular Institute, The Wireless Foundation, D.C.-area Hospitals and D.C. Fire & EMS have partnered to reduce time from onset of chest pain to treatment by equipping D.C.-area ambulances with technology that enables rapid, wireless transmissions of EKGs to both the on-call physician's wireless device and tertiary care hospitals. See <http://www.newswise.com/articles/view/596059/>.

²² See, e.g., <http://www.ihealthbeat.org/features/2012/meaningful-use-stage-3-could-include-patientgenerated-health-data.aspx>;

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

TIA believes that benefits can be derived from existing regulatory mechanisms. Flexible, bottom-up approaches using appropriately granular risk assessments will provide much-needed certainty in the health IT field generally, and will facilitate competition and innovation. Factors that should be included in current and any future risk-based regulatory approach to health IT should promote innovation and protect patient safety by including:

- **Clear and common definitions.** Within an agency's regulations and guidance, it is very important that key terms and taxonomy be clearly defined. Depending on the agency and even the matter within an agency, different terms and phrases may have different definitions. When encountered in the product development process, particularly in the early stages of that process, finding differing meanings for the same phrases and terms in Federal laws or agencies is a clear deterrent to innovation. FDA, ONC, FDA, and others should collaborate in each agency's development of regulatory definitions to ensure that this barrier does not arise.
- **Answers to key questions to increase regulatory clarity.** From the largest corporation to the solo innovator, investing in research and development is a risk. These risks do not always work out, but have led time and time again to advances in all aspects of technology, including health IT, which have great societal benefits. The U.S. government, in crafting a risk-based regulatory approach for health IT, will need to continue to enhance the level of regulatory certainty to truly promote innovation and protect patient safety. TIA believes that clarity is particularly needed – collectively by the FDA, ONC, FCC, and others – to settle the following important questions, among others:

- Which agencies oversee the legal marketing of mobile health IT applications, and in what capacity (scope, regulatory approach) and how do they interact?
- What criteria and requirements are employed in the health IT product approval process by respective agencies?
- Can regulatory clarity on converged medical devices and general guidance on all relevant topics be expedited from each respective agency that oversees the marketing and availability of such devices? Where can exemptions from good manufacturing practices or quality systems regulations be appropriately applied and noticed (e.g., certain Class I and Class II devices under the FDA)?²³ Where can “Enforcement Discretion” be appropriately applied when regulation of a known low-risk medical device is inappropriate?
- How are relevant agencies collaborating, information sharing and coordinating activities relative to health IT, including mobile medical applications?
- What external facing resources are each agency utilizing to educate the industry and public about health IT and regulatory treatment of these technologies?

As noted above, excellent first steps towards providing concrete answers can be accomplished by the FDA’s establishment of policies of “enforcement discretion” for lowest-risk health IT. In addition, significant clarity would be provided through providing an exemption from GMP for lower-risk health IT.

- **A realization of the full potential of open, voluntary, and consensus-based standards.** SDOs including TIA develop open, voluntary standards that emphasize consensus positions under a transparent process. The Federal government should support the use of these standards and participate in their development.
- **Technology neutrality.** TIA believes that a risk-based regulatory approach for health IT to promote innovation and protect patient safety includes the key concept of “technology neutrality” – that the government set objectives in its policies, but avoid

²³ See Good Manufacturing Practices (“GMP”) in 21 CFR Part 820.

dictating, in all possible cases, how those objectives are met. Not only does this promote innovation, but it prevents favoritism of one solution or company over others, , and in this way enhances competition. We believe that the agencies at issue in this matter appreciate the benefits of technology- and platform-agnostic approaches.²⁴

- **A holistic approach when balancing risks and benefits, under a “prescriptive/inclusionary” focus.** TIA recommends that FDA, ONC, FCC, and others, in determining the scope and assessment process, appropriately weigh the manner in which a product is marketed, the product’s functionality, and the level of risk that product poses based on the product’s intended use but also its use case . This determination, under a “prescriptive/inclusionary” approach where categories of health IT deemed appropriately regulated are explicitly listed as “in-scope” and others not named are presumed “out-of-scope,” could provide much needed relief from the high-liability legal issues surrounding potential health IT regulation. However, for those devices which are “in-scope,” we urge that the degree of risk presented to patient health by the device as well as its use in given circumstances dictate the amount of oversight and regulation. For example, a majority of Class I medical devices, the FDA exercises exemption from GMP. For low-risk level Class I health IT, an exemption from GMP should be considered.
- **Clear regulation and guidance on accessories.** A key modality for innovation in health IT devices falls under the category of accessories. Accessories have the ability to augment a device’s effectiveness in many ways which do not affect the level of risk that the parent or accessory device pose to patient safety, such as an accessory that extends the battery life of a device or any other improvement that does not implicate Section 201(h) of the FD&C. We strongly urge the FDA to make clear how health IT accessories will be treated in interoperable, systematic virtual environments.

²⁴ For example, as far back as 1997, the FCC has stated that “Technological neutrality will allow the marketplace to direct the advancement of technology and all citizens to benefit from such development. By following the principle of technological neutrality, we will avoid limiting providers... to modes of delivering that service that are obsolete or not cost effective. Federal-State Joint Board on Universal Service, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776 (1997), ¶ 49.

3. 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.*

FCC & FDA – Device Approval for Marketing/Sale: The FCC approves all Part 68 terminal equipment²⁵ and RF-emitting devices²⁶ before they can be legally marketed or sold in the U.S.; the FDA approves medical devices and radiation-emitting products,²⁷ including those which may either fall under the definition of Part 68 terminal equipment or be wireless, before marketing or sale in the U.S. is allowed.

FCC & FDA – Radio Frequency Interference: The FCC approves all RF-emitting devices before they can be legally marketed or sold in the U.S.,²⁸ and this approval process specifically includes attestation of and testing to interference mitigation. The FDA issues guidance on pre-market approvals of devices, including those which may be wireless, and specifically addresses RF-based interference (for example, in draft guidance on pre-market submissions for “home use” device approvals, the FDA has stated that “[c]ompliance of RF wireless technologies with applicable technology standards and [FCC] rules does not necessarily alleviate home use device

²⁵ See 1998 Biennial Regulatory Review -- Amendment of Parts 2, 25 and 68 of the Commission's Rules to Further Streamline the Equipment Authorization Process for Radio Frequency Equipment, Modify the Equipment Authorization Process for Telephone Terminal Equipment, Implement Mutual Recognition Agreements and Begin Implementation of the Global Mobile Personal Communications by Satellite (GMPCS) Arrangements, GEN Docket No. 98-68, *Report and Order*, 13 FCC Rcd 24687 (1998).

²⁶ See 47 C.F.R. Part 2 Subpart J.

²⁷ See 21 U.S.C. 321(h); and 21 CFR Parts 800-1299.

²⁸ See 47 C.F.R. Part 2 Subpart J.

safety and effectiveness concerns.”)²⁹. Furthermore, final guidance on RF wireless technology in medical devices has been pending since 2007.³⁰

FCC & ONC – EHRs: The FCC’s Health Care Connect Fund provides funding for broadband services and equipment to facilitate telehealth services, which the FCC notes to include “exchange of [EHRs]; collection of data through Health Information Exchanges and other entities,” among other things; ONC develops standards and certification related to how eligible providers accomplish the meaningful use of health IT while CMS provides requirements and the actual incentive payments to eligible providers to encourage the adoption of health ITs.³¹

FCC, FDA & ONC – Security/Cybersecurity: The FCC, FDA, and ONC – along with a number of other Federal agencies including the Federal Trade Commission;³² Centers for Medicare & Medicaid Services (“CMS”)³³ and HHS Office of Civil Rights (“OCR”)³⁴ (note that OCR oversees and enforces the Privacy Rule, while CMS oversees and enforces all other Administrative Simplification requirements, including the Security Rule); National Institute of Standards and Technology (“NIST”);³⁵ and Securities Exchange Commission³⁶ – all have efforts to address

²⁹ See FDA, *Draft Guidance for Industry and Food and Drug Administration Staff; Mobile Medical Applications; Availability*, 76 Fed. Reg. 43,689 (July 21, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-07-/pdf/2011-18537.pdf>, at 15.

³⁰ See <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm>.

³¹ See *In the Matter of Rural Health Care Support Mechanism, Report & Order*, WC Docket No. 02-60 (rel. Dec. 21, 2012).

³² The FTC requires vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached. See <http://www.gpo.gov/fdsys/pkg/FR-2009-08-25/pdf/E9-20142.pdf>.

³³ See 45 CFR Part 160 and Part 164, Subparts A and C.

³⁴ See 45 CFR § 160.103.

³⁵ NIST sets computer security standards for the federal government and publishes reports on topics related to IT security. See <http://csrc.nist.gov/>.

³⁶ The SEC has issued guidance on the disclosure obligations relating to cybersecurity risks and cyber incidents. See <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

device or network security and cybersecurity issues. All have direct impacts on health IT manufacturers and vendors.

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?

All (FCC, FDA, ONC)

- As discussed above, each agency addresses different – though sometimes overlapping – areas of health IT. Each agency should ensure that, when appropriate, it is aware of, and when necessary participates in, the regulatory process of the other agencies. In addition, agencies should include in their considerations state and local regulations to prevent duplicative or conflicting requirements. For example, in the FDA’s request for public input on its draft “home use” guidance, the FCC should have participated in this proceeding, and clarified its views on its own roles and responsibilities – including where it defers to the FDA – in the mitigation of interference. The mHealth Task Force has already recommended in September 2012 that FCC, ONC, and CMS should seek a closer collaboration related to ongoing health IT and information exchange efforts.³⁷ This effort should also build on and integrate the existing informal FDA-sponsored Medical Device Interoperability Coordination Council (“MDICC”), which aims to allow “collaboration between stakeholders that are actively engaged in aspects of promoting or creating interoperable medical device systems.”³⁸ A straightforward way to address this coordination quandary is for a joint memorandum of understanding (“MOU”) to be agreed to across the agencies, such as the MOU entered into between the FCC and FDA

³⁷ See mHealth Task Force Recommendation 2.3, available at <http://www2.itif.org/2012-mhealth-taskforce-recommendations.pdf>.

³⁸ See, e.g., http://www.mdpnp.org/MD_PnP_Program_Projects.html. The MDICC does not currently include the FCC.

in 2010.³⁹ We believe that the discussion required to reach agreement on the language of such a MOU would facilitate valuable conversation towards coordinated, appropriate regulatory approaches.

All (FCC, FDA, ONC)

- As described above, FCC, FDA, ONC have all undertaken some form of activity to address security- or cybersecurity-related concerns. While not *all* activities are “regulations,” they at least inform the development of regulations by one or more of the agencies, and certainly affect industry product development decisions. Depending on the agency and its authority, whether it is concretely proper to partially or fully address security and/or cybersecurity issues will vary. Furthermore, the Executive branch is currently undertaking a massive effort to improve cybersecurity in both the Federal government as well as the private sector.⁴⁰ A number of proposals exist (and are expected) in Congress. Any efforts to improve security and cybersecurity in the health IT space should be coordinated and complimentary amongst FDA, ONC, and FCC, and should where possible rely on industry-led, voluntary, and consensus-based standards.

FCC & FDA

- In collaboration with the FDA as well as the Environmental Protection Agency and Occupational Safety Administration, and numerous other public and private stakeholders, the FCC has established RF standards applicable to all wireless devices marketed, sold, or distributed in the United States. In addition, the FCC is statutorily responsible for spectrum management policies that encourage new technologies and

³⁹ See, e.g., MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL COMMUNICATIONS COMMISSION AND THE FOOD AND DRUG ADMINISTRATION CENTER FOR DEVICES AND RADIOLOGICAL HEALTH (2010), available at http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0726/DOC-300200A2.pdf.

⁴⁰ See Executive Order—Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013.

services, ensure efficient use of spectrum, and protect licensees from harmful interference.⁴¹ The testing that all products authorized by the FCC must undergo ensures that devices will operate safely and share spectrum successfully with other users, including devices that operate in the same frequency range. Even in unlicensed (Part 15) frequencies, where uses are subject to the conditions that no harmful interference is caused and that interference must be accepted,⁴² the FDA and others should defer to the requirements of the FCC in making their determinations on the appropriateness of use. In other words, the FDA should not make necessary separate RF interference testing in order to attain FDA approval for a wireless medical device or application, and should rely on the FCC for the management of harmful interference.

FCC & ONC

- While the FCC's Health Care Connect Fund provides discounts on broadband services, equipment, connections, the HITECH Act provides incentive payments for the adoption of electronic health records (ONC sets rules, and CMS "enforces" them via attestations). FCC's Universal Service Administrative Company ("USAC") and ONC should ensure that these two programs do not support duplicative purchases or services or equipment in order to maximize the reach and effect of both programs. At the same time, where a healthcare provider or other entity is eligible for both programs and does receive this assistance from both programs, FCC and ONC/CMS will be able to complement one another in furtherance of each agency's mission. The mHealth Task Force also has recommended that the FCC "be consulted and be invited to have representation during ongoing rulemaking efforts, including ONC federal advisory committee meetings, related to the Medicare and Medicaid EHR incentive program and the development of

⁴¹ See 47 U.S.C. § 303(f)-(g).

⁴² See 47 C.F.R. § 15.5(b).

standards and certification criteria for EHR technologies.”⁴³ We suggest that these agencies voluntarily undertake this effort.

All (FCC, FDA, ONC)

- There is confusion of varying levels among Congress, regulators, stakeholders, and the general public as to the state of health IT governance, about which agency plays which role, and the effect of government’s activity in this area on the availability and innovative development of health IT products and services. In reports pursuant to the FDASIA, the public reports should address these topics in a straightforward way, and include commitments from FCC, FDA, and ONC to increase outreach and educational efforts, consistent with the above.

⁴³ mHealth Task Force Findings and Recommendations (Sept. 2012) at 7.

III. Conclusion

TIA, on behalf of the health IT manufacturing and vendor community, requests that its views in this matter be considered and stands ready to work with the Federal government as it moves forward in health health IT reform.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: /s/ Danielle Coffey__

Danielle Coffey

Vice President & General Counsel, Government
Affairs

Brian Scarpelli

Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

10 G Street N.E.

Suite 550

Washington, D.C. 20002

(202) 346-3240

August 31, 2013