Testimony before the Subcommittee on Oversight and Investigations
Committee on Energy and Commerce

U.S. House of Representatives

Statement of

Farzad Mostashari, M.D., ScM.

National Coordinator, Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services

Health Information Technologies:
Administration Perspectives on Innovation and Regulation
March 21, 2013

Chairman Murphy, Ranking Member DeGette, and distinguished Subcommittee members, thank you for the opportunity to appear today on behalf of the Department of Health and Human Services (HHS). My name is Dr. Farzad Mostashari and I am the National Coordinator for Health Information Technology.

In 2009, Congress and President Obama enacted the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Reinvestment and Recovery Act of 2009 (ARRA). HITECH established the Office of the National Coordinator for Health Information Technology (ONC) by law and provided the resources and infrastructure needed to stimulate the rapid, nationwide adoption and use of health IT, especially electronic health records (EHRs). Among other measures, HITECH included the establishment of the Medicare and Medicaid EHR Incentive programs which provide technical assistance and financial incentives to eligible professionals and hospitals that adopt and "meaningfully use" EHRs.

Thank you for the invitation to be here today to discuss how health IT benefits patients and provides the tools that are necessary to transform care. Already, HHS and its partners have made significant progress expanding health information technology use. Since 2009 physician EHR adoption has nearly doubled, growing to 40 percent in 2012, and hospital EHR adoption has more than tripled over the same period, increasing to 44 percent. In addition, I would like to provide a status report on HHS's Patient Safety Action & Surveillance Plan and an update on the progress we have made in the relatively short time since HITECH's passage. Finally, I will conclude with an overview for what we have planned in 2013 and beyond.

Health IT is Transforming Care

Technology is just a tool - but it is a critical tool that can foster much-needed innovation in entrenched industries. Our healthcare system is poised for a transformation in how care is paid for and delivered and how patients engage in their own health and health care. Health information technology supports these transformations.

In the past, our healthcare delivery system based its payments solely on the number of services provided and not on the quality of care. As a result, patients might receive duplicative tests and/or services that might not improve their health. As required by the Affordable Care Act, HHS has launched several initiatives to more closely link payments with quality outcomes and promote value-based care.[1] For example, the hospital readmissions reduction program links hospital payments in Medicare to avoidance of potentially preventable readmissions. These reforms enable HHS to promote value over volume, and patient safety, and ensure that care is better coordinated across the healthcare delivery system.

As both public and private payers take concrete steps to change the incentives for paying providers, health IT can provide the infrastructure for improved care coordination, better quality, and lower costs, as well as the data analytics that providers need to understand the cost of doing business under the new payment models.

[1] See Statement of Jonathan Blum on Delivery System Reform: Progress Report from CMS: Senate Committee on Finance, February 28, 2013.

Federal Advisory Committees: The HIT Policy and Standards Committees

Recognizing that health IT is a complex and quickly changing field, HITECH established two Federal advisory committees under the Federal Advisory Committee Act (FACA). The Health IT Policy Committee was created to make recommendations on a policy framework to support the development and adoption of a nationwide health information infrastructure. The Health IT Standards Committee is responsible for making recommendations on standards, implementation specifications, and certification criteria for the use and exchange of health information.

Both the HIT Standards Committee and HIT Policy Committee include experts from the private sector to help guide ONC and the Centers for Medicare & Medicaid Services (CMS) in developing the rules for meaningful use and the certification of EHR technology. HITECH specified the different stakeholder perspectives that must be represented on the Committees. The law explicitly charged the Comptroller General of the United States with the responsibility of appointing 13 members representing various stakeholder groups to the Health IT Policy Committee. Additional perspectives are provided by the members appointed by the Secretary of Health and Human Services, the Majority and Minority Leaders of the Senate, and the Speaker and Minority Leader of the House of Representatives. HITECH further specified that the Health IT Standards Committee include providers, ancillary healthcare workers, consumers, purchasers, health plans, technology vendors, researchers, relevant Federal agencies, and individuals with technical expertise on health care quality, privacy and security, and health information exchange.

To further enrich the advice they provide, each Committee maintains several workgroups that incorporate the perspectives of additional stakeholders from government and the private sector. Since the creation of the Committees, their members and their many working groups have dedicated their time to meeting an average of once every other day for the past three years. We make each Committee's meetings publicly available through live webcasts. These Committees have informed the development and implementation of all of HITECH initiatives.

Progress on HITECH Implementation

Our goal is to assist clinicians and hospitals in using technology to meaningfully deliver health care that is higher quality, safer, patient-centered, and coordinated. And, we want providers to thrive in the new health care marketplace that puts a premium on value over volume, on coordination over fragmentation, and on patient-centeredness over all.

The CMS Medicare and Medicaid EHR Incentive Programs, the ONC-led certification program for electronic health records, as well as the hands-on technical assistance provided by the Regional Extension Centers (RECs) across the country, are critical in facilitating unprecedented progress in EHR development, adoption and use. There are over 1,700 unique certified products produced by nearly a thousand developers, and certified by one of five ONC-accredited private sector certification bodies. As of February 2013, more than 230,000 providers -- nearly 43 percent of the nation's eligible professionals, and over 75 percent of eligible hospitals -- have earned over $12.6 billion in total payments for meeting the requirements of the EHR Incentive Programs. ONC's Regional Extension Centers (RECs) have

signed up more than 130,000 primary care providers in over 30,000 different practices. This means that roughly 44% of the nation's primary care providers have committed to meaningfully using EHRs by partnering with their local REC. RECs have signed up more than 20,000 Nurse Practitioners (NPs), 48% of all NPs nationwide, to assist them in meaningfully using EHRs. More than 80% of all Federally Qualified Health Center grantees are enrolled with an REC.

Health IT Patient Safety Action and Surveillance Plan

The Institute of Medicine's (IOM's) 1999 landmark report *To Err is Human* raised awareness of the large number of avoidable medical errors harming patients. The report also stated that the use of information technology could improve patient safety through automated order entry, clinical reminders, and drug - drug interaction and drug - allergy checking. While the magnitude of establishing a national infrastructure was hard to imagine in 1999, the Medicare and Medicaid EHR Incentive Program is a realization of that goal. Health IT – which includes EHRs and health information exchange – has already demonstrated the ability to reduce medical errors. For example, EHRs can flag and help providers avoid potential drug-drug interactions and improve the accuracy of physicians' drug ordering. Yet health IT will only fulfill its enormous potential to improve patient safety if the risks associated with its use are identified, if there is a coordinated effort to mitigate those risks, and if it is actually used to make care safer.

Recognizing the need to understand how health IT can promote patient safety as well

as identify and mitigate risks, ONC commissioned an IOM study to determine how government and the private sector working collaboratively can maximize the safety of health IT-assisted care. The IOM report, *Health IT and Patient Safety: Building Safer Systems for Better Care*, was published in November 2011.

The IOM Report included the following three key findings:

- Health IT can improve patient safety in some areas such as medication safety; however, there are significant gaps in the literature regarding how health IT impacts patient safety overall;
- Safer implementation and use begins with viewing health IT as part of the larger sociotechnical system;
- All stakeholders need to work together to improve patient safety.

Based on these findings, the IOM recommended that the market forces are not adequately addressing the potential risks associated with the use of health IT and all stakeholders must coordinate efforts to identify and understand patient safety associated with health IT.

Building on IOM's recommendations, ONC worked collaboratively with colleagues throughout HHS to develop the *Health IT Patient Safety Action and Surveillance Plan,* the draft of which was released on December 21, 2012. This *Health IT Safety Plan* addresses the role of health IT within HHS' commitment to patient safety. The plan seeks to build upon and strengthen patient safety efforts across government programs and in the private sector – including efforts by patients, health care providers, technology companies, and health care

oversight bodies – to improve knowledge on health IT-related patient safety events.

The draft plan prescribes actions that all stakeholders can take within their existing authorities and resources to promote a culture of safety related to health IT. Suggested actions include:

- Use ONC-Authorized Testing and Certification Bodies to collect complaints and conduct surveillance;
- Work with developers to establish a code of conduct that includes working with Patient Safety Organizations and supporting providers in reporting adverse events;
- Work with Patient Safety Organizations according to the Agency for Healthcare Research and Quality's (AHRQ's) Common Formats in order to improve aggregation and analysis of reported events;
- Include safety requirements related to user-centered design, quality management systems, and easier reporting of adverse events in ONC regulations;
- Work with CMS to train surveyors and use health IT to assist investigations;

ONC received public comments on the draft plan through February 4, 2013, and those comments have been generally favorable. We are in the process of reviewing comments and will publish the final Health IT Safety Plan in the near future.

Consumers – The Most Underutilized Resource in Healthcare

Over the past few decades, we have seen information technology improve the consumer experience in almost every other aspect of our lives, including the way we manage our finances, shop, and book travel. But, health care has been slower to leverage this technology. Most notably, relevant information is not available to patients when and where it is needed.

Increasingly, people are literally taking their health into their own hands—whether that means tracking their health through a Smartphone app or a remote monitor, participating in online patient or caregiver communities, or accessing their medical records online. Changes in consumer technology, such as the growth of mobile phones, are helping to drive this change -- nearly nine out of ten people own a mobile device and nearly half of all Americans own a smartphone.[2] Mobile devices offers several advantages over traditional PCs—they can help remove traditional barriers such as geography and time, breaking down the digital divide in underserved communities, enabling remote treatment, and more continuous monitoring of health make health more convenient and personalized. The mobile devices in our pocket can help us access a world of information at the right time to help make the right health decisions, which is important since 80% of Internet users have gone online seeking health information.[3] Apps like iTriage can help us find a local care facility and Pillbox can help us quickly identify unlabeled medications. iBlueButton – developed pursuant to an HHS-sponsored challenge

[2]Pew: http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012/Main-Findings/Cell-Internet-Use.aspx

[3] Pew: http://www.pewinternet.org/Reports/2011/HealthTopics.aspx).

program – can help us share our medical history, and Ginger.io tracks our level of activity. The Department of Defense has developed apps to help veterans and their caregivers cope with post-traumatic stress disorder. Mobile phones can be an incredible tool for empowering consumers to take control of their health, their care, and their healthcare finances and as we know from the literature, more engaged consumers get better outcomes.

ONC's strategy in consumer eHealth is to work with partners to increase patients' ability to access their own health data, to increase the use of this data for actionable apps and services, and to shift attitudes around patient empowerment.

ONC is also encouraging institutions that have health data to make it easier for patients to get easy, electronic access to their data and to use that information in ways that improve their health and health care. The Blue Button Pledge Program is a voluntary mechanism for supporting consumers' access to their health data. The Blue Button Pledge Program now includes more than 450 organizations that are committed to learning and collaborating in efforts to increase patient access to, and use of, health data. The Pledge Program, launched in 2011, includes "data holders"—such as health care providers and insurers—who pledge to improve the accessibility of health data to patients and other authorized users, and "non–data holders"—such as software developers and consumer advocacy organizations— who pledge to educate consumers about the value of getting and using their health data.

The government is moving forward in this direction. Veterans today can access their full records online, and download their records with a simple click of a "Blue Button"- and more than one million veterans have done so. Medicare beneficiaries can access their full Medicare records online today, and download three years of claims data. HHS is also encouraging

Medicare Advantage plans to expand the use of Blue Button to provide beneficiaries with one-click secure access to their health information. And the Federal Employee Health Benefits program has asked carriers to do the same.

Our regulations and guidance are also encouraging this "data liberation" to patients and consumers. Our partners in HHS's Office for Civil Rights (OCR) recently launched a campaign to build public awareness of individuals' legal right under the Health Insurance Portability and Accountability Act of 1996 Privacy Rule to access their own health information – including an electronic form – if the information is readily producible in the form. In May 2012, OCR released a memo detailing these rights and directing consumers to educational resources.

Meaningful Use Stage 2, as part of the Medicare and Medicaid EHR Incentives Programs, requires eligible providers to use secure e-mail with patients and to provide patients with a way to view, download, and transmit their own health information. Under Stage 2, patients will be able not only to view their health information online, but also to export their data from EHRs in structured and human-readable formats; share those data with others; and use tools and applications to store, analyze, or otherwise make use of their information. Stage 2 also establishes thresholds for the proportion of patients using these functions, which will encourage providers to promote their use.

Privacy and Security of Mobile Technology (including Mobile Applications)

At ONC, we recognize that clinicians want to use mobile technology to access and transmit health information in health care delivery. We recognize the mobile device benefits – portability, size, and convenience in overall care coordination.

However, we recognize that there are risks as well as benefits to any technology. The use of mobile health technology holds great promise in improving health and health care. But the ubiquity and connectedness of mobile devices creates concerns for privacy and security. ONC has developed a number of projects that address the privacy and security of mobile health (mHealth) devices, including convening stakeholders and focus groups to identify concerns and developing technical assistance and education materials to begin to address those concerns.

First, ONC is working with other agencies and stakeholders to identify security issues with regard to mHealth technology, including smartphones, implantable medical devices, and remote monitoring devices. As part of this assessment, ONC hosted the public Mobile Device Roundtable in March 2012 where we gathered public, industry, health care provider, and subject matter expert input on the topic of safeguarding health information when using mobile technology.[4] The Roundtable included participants from various federal bodies that have a role in mobile health, including the Food and Drug Administration (FDA), the Federal Communications Commission (FCC), FTC, and OCR, to discuss the current privacy and security

[4] For more information about the Mobile Device Roundtable, please visit: http://www.healthit.gov/policy-researchers-implementers/mobile-devices-roundtable-safeguarding-health-information

legal framework for mobile devices accessing, storing, and transmitting health information. In addition, through its mHealth Privacy and Security Consumer Research Initiative, ONC identified and explored consumer attitudes and preferences, including underserved populations and different age categories, regarding the privacy and security of communicating health information using mobile devices, including the use of mobile apps.[5] The research initiative highlights the important role that technology developers can play in meeting consumer needs for functionality and improving privacy and security. Results from the initiative may help inform future policy and educational development activities.

Second, based on these assessments, ONC has developed technical assistance materials on privacy and security involving mobile technology. For example, in December 2012, ONC and OCR rolled out a national, multi-prong privacy and security educational initiative targeted at health care providers and professionals using mobile devices such as laptops, tablets, and smart phones in the delivery of care.[6] We developed a set of online tools that encourage health care providers and professionals to know the risks and take the steps to protect and secure health information when using mobile devices. These materials are available at https://www.healthIT.gov/mobiledevices. Although the materials were developed with health care providers in mind, anyone can use the education materials to help them securely adopt and harness the power of these technologies.

Through these projects, ONC has been able to rapidly assess and respond to the growing

[6] A variety of resources, including videos, fact sheets, and other downloadable resources, addressing the privacy and security protections and safeguards can be found here: http://www.healthit.gov/mobiledevices

need for privacy and security policy and guidelines in securing health information as it is being stored and transmitted through mobile technology.

Model Personal Health Record Privacy Notice

As personal health information increasingly becomes stored managed by companies that offer direct-to-consumer technologies, it becomes important for consumers to be aware of these companies' data practices, and to have an easy way to compare the data practices of two or more companies.

The Personal Health Record (PHR) Model Privacy Notice is designed to be a standardized template that a web-based PHR company can use to succinctly inform consumers about its privacy and security policies[7]. The PHR Model Notice was developed by ONC based on consumer testing that identified key issues individuals care about and language that they understand. The PHR Model Privacy Form is meant to be similar to other consumer-oriented "labels" that have been developed for other industries, such as the nutrition facts label for food, and the Model Privacy Notice developed for the financial services industry for compliance with the Gramm-Leach Bliley Act. It is intended to focus only on some important information and does not substitute for more comprehensive privacy policies. Many of the largest PHR companies have agreed to use the PHR Privacy Model Notice. ONC does not enforce use of the tool. However, if a PHR company under the jurisdiction of the Federal Trade Commission

[7] http://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice

(FTC) does not adhere to the privacy and security commitments stated in their PHR Notice, the FTC has the authority to challenge the notices as false or misleading in violation of the Federal Trade Commission Act. [8]

FDASIA Workgroup on Risk-Based Regulatory Framework for Health IT

Throughout the development of the *Health IT Patient Safety Action and Surveillance Plan*, ONC worked collaboratively with other federal agencies such as the Agency for Healthcare Research and Quality (AHRQ), CMS, FDA, and FCC to leverage existing authorities and to add a focus on health IT and patient safety. On February 20, ONC, FDA, and FCC announced the formation of the Food and Drug Administration Safety Innovation Act (FDASIA) Workgroup – under ONC's Health IT Policy Committee -- to provide expert for the development of a Congressionally-mandated report on an appropriate, risk-based regulatory framework pertaining to health IT, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication.[9] FDASIA indicated that if a

[8] For a more complete explanation of how the voluntary adoption of privacy and security practices can result in legally enforceable commitments, see The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Global Digital Economy, Feb. 2012, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. In addition, the National Telecommunications and Information Administration is convening stakeholders to develop a code of conduct to improve transparency in how mobile applications collect, store, and use personal data. *See* https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[9] Section 618 of the 2012 FDASIA charges the Secretary of Health and Human Services (the Secretary) (acting through the Commissioner of the Food and Drug Administration (i.e., FDA), in consultation with the National Coordinator for Health Information Technology (i.e., ONC) and the Chairman of the Federal Communications Commission (i.e., FCC) to publish a report by January 2014 that expresses "a proposed strategy and

workgroup was formed, it should be geographically diverse and include representatives of patients, consumers, health care providers, startup companies, health plans or other third-party payers, venture capital investors, information technology vendors, health information technology vendors, small businesses, purchasers, employers, and other stakeholders with relevant experience. The three agencies received applications through March 8th to participate in the Workgroup and are now in the process of reviewing the nominations. The first meeting of the workgroup is expected to be held in April 2013.

The FDASIA Workgroup will build on prior work such as the IOM report, *Health IT and Patient Safety: Building Safer Systems for Better Care and ONC's Health IT Patient Safety Action and Surveillance Plan*; FDA's mobile medical applications guidance[10] and *Medical Device Data Systems Rule*[11]; FCC's *National Broadband plan* and other relevant work. Specifically the three agencies will seek input on issues relevant to the report:

- Types of risk that may be posed by health IT which impact patient safety, the likelihood that these risks will be realized, and the impact of these considerations on a risk-based approach;

recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication."

[10] FDA's proposed oversight approach would limit FDA oversight of mobile medical apps to the small subset that are either used as an accessory to a regulated medical device, or that transform a mobile platform into a regulated medical device.

[11] This is a down classification rule (Class I) that does not require premarket submissions for medical products that are intended to be used in diagnosing, curing treating of a disease and that transfer, store, convert formats, and display medical device data.

- Factors or approaches that could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety; and
- Approaches to avoid duplicative or overlapping regulatory requirements.

Like all ONC FACA Workgroups, all FDASIA Workgroup meetings and documents discussed at the meetings will be publicly available and will offer opportunities for public comments.

Conclusion

New technologies – including health IT and mobile applications – offer great promise to improve the quality of care and bring down health care costs. Our progress in moving towards these goals has been steady and deliberate. Working within an open and transparent process with our public and private stakeholders, we have developed a health IT patient safety and surveillance report.

We have worked with other government agencies to help secure the privacy of mobile applications, within existing authorities whenever possible. As technologies continue to advance, we want to work together with Congress to ensure health data is secure.

To truly transform delivery, health care providers must also redesign and reengineer workflow of care. This does not happen overnight. Health IT holds tremendous promise for delivering "smart health" to patients right at their fingertips to help all of us achieve the best possible outcome for each individual. We must carefully balance the need for the widest innovation possible, with protection of patient privacy, security, and safety.

We look forward to continuing to working with Congress to accomplish these goals. I would be happy to answer any questions that you may have regarding my testimony.