July 7, 2014

Leslie Kux
Assistant Commissioner for Policy
Food and Drug Administration
Division of Docket Management (HFA–305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: Docket No. FDA–2014–N–0339: Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report; Request for Comments

Dear Ms. Kux,

The Bipartisan Policy Center (BPC) appreciates the opportunity to comment on the proposed risk-based regulatory framework and strategy for health information technology (IT), as summarized in the *FDASIA Health IT Report: Proposed Strategies and Recommendations for a Risk-Based Framework* (FDASIA report). We also appreciated the opportunity to participate in the May 2014 public workshop related to this work.

Established by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole, and George Mitchell, BPC is a nonprofit organization that drives principled solutions through rigorous analysis, reasoned negotiation, and respectful dialogue. BPC's Health Innovation Initiative engages experts and stakeholders, advancing recommendations that promote innovation and the use of IT to drive improvements in the cost, quality, and patient experience of care.

We commend the Food and Drug Administration (FDA), the Office of the National Coordinator for Health IT (ONC), and the Federal Communications Commission (FCC) (the Agencies) for their public process and dedicate work associated with the FDASIA report.

We believe that the proposed risk-based regulatory framework and strategy outlined in the FDASIA report is generally the right approach for protecting patient safety and continuing to promote innovation in the development, implementation, and use of health IT. We are pleased to see the inclusion of numerous BPC recommendations in the draft FDASIA report. BPC engaged hundreds of experts and stakeholders across every sector of health care in the development of a set of principles and recommendations for a risk-based regulatory framework for health IT which are captured in the report, *An Oversight Framework for Assuring Patient Safety in Health Information Technology* (BPC report).

Our comments on the FDASIA report are summarized below.

Health IT: Lifecycle and Sociotechnical Considerations

The Agencies' approach, which focuses on the entire health IT lifecycle and takes into consideration the fact that health IT is part of a larger sociotechnical system, is in significant alignment with the principles and assumptions laid out in the BPC report.

We agree with the Agencies' observation that the safety of health IT relies not only on how it is designed and developed, but also on how it is customized, implemented, integrated, and used. We also concur that the health IT life cycle includes design and development; implementation, customization, and integration; and post-deployment (which includes upgrades, maintenance, operations or use, surveillance, reporting, risk mitigation, and remediation).

We also agree with the Agencies' recognition that health IT is part of a larger sociotechnical system that includes people, health care organizations, health IT developers and vendors, processes (actions and procedures performed during the delivery of health care), and the environment of use. Therefore assuring patient safety is a shared responsibility that must involve the entire health care system.

Focus of the Proposed Strategy and Recommendations for a Risk-Based Regulatory Framework

Throughout the FDASIA report, the Agencies' proposed strategy and recommendations are based on the premise that risk and corresponding controls should focus on health IT functionality—not the platform(s) on which such functionality resides or the product name/description of which it is a part. The Agencies' strategy and recommendations seek to advance a framework that is sufficiently flexible to accommodate the future and rapid evolution of health IT. We agree with both concepts which are consistent with the BPC report.

We also concur with the Agencies' identification of at least three categories of health IT, including administrative, health management, and medical device functionalities. A similar framework was outlined in the BPC report.

We generally concur with the Agencies' categorization of various functionalities within the framework. We also concur with the Agencies' observation that the systems that health care organizations purchase often contain functionalities that bridge all three categories.

The Agencies' recognition that only health IT with medical device functionality should be the focus of FDA's oversight and that health IT with administrative functionality should not be subject to any additional oversight, is consistent with the recommendations in our report.

We also concur with the Agencies' recognition that health IT with health management functionality should be subject to a risk-based framework that (1) promotes the use of quality management principles, standards, and best practices; (2) leverages conformity assessment tools such as product testing, certification and accreditation; and (3) creates an environment of learning and continual improvement. All of these concepts are consistent with those outlined in the BPC report. More detailed comments on each of these elements are provided below.

As the Agencies move forward with the implementation of several aspects of the FDASIA report, it is critically important that they more clearly define the criteria that would govern placement of health IT within one of the three categories. The BPC report states that functionalities should be assessed principally by their potential to harm a patient as well as the degree to which a health care professional has a reasonable opportunity to intervene.

Proposed Strategy and Recommendations for a Health Management Health IT Framework

The Agencies propose that health IT with health management functionality should be addressed through a risk-based framework that adheres to the following principles:

- Employ a risk-based (and evidence-based) approach to appropriately mitigate patient safety risks while avoiding unnecessary regulatory oversight;
- Leverage private sector knowledge, experience, and expertise;
- Facilitate, rather than impede, innovation;
- Promote transparency of product performance and safety; and
- Create/support an environment of learning and continual improvement.

These principles are consistent with those noted in the BPC report.

Promote the Use of Quality Management Principles; Identify, Develop, and Adopt Standards and Best Practices

We concur that the application of quality management principles, including a quality systems approach by health IT stakeholders, is necessary for the safe design, development, implementation, customization, and use of health IT. We also concur that the identification, development, and adoption of standards and best practices are a key aspect of a health IT framework that promotes innovation and protects patient safety. Both concepts are in significant alignment with the BPC report.

In addition, we offer the following comments, drawn from an April 2014 letter developed by BPC, Health IT Now, and HIMSS and agreed upon by a diverse group of stakeholders.

1. There should be a single national approach for identifying and gaining consensus on a broad and flexible set of standards that can be applied to a diverse range of processes, products, and settings (including those that span the three categories of health IT).

2. Such an approach should reflect good governance practices and promote public participation.

3. The national standards consensus process should demonstrate the attributes of a "voluntary consensus body", which are defined by OMB Circular A-119 to include openness, balance of interest, due process, and appeals process, and consensus.

4. The national standards consensus process should engage both public and private stakeholders, including but not limited to experts in patient safety, health IT, health informatics and information management, as well as clinicians, clinics, consumers, employers, health plans, hospitals and health systems, laboratories, medical device manufacturers, mobile technology companies, patient safety organizations, pharmacies, health IT companies, and the many federal and state agencies that play a role in patient safety and/or the development, implementation, or use of IT in health care.

5. The National Technology Transfer and Advancement Act of 1995 and OMB Circular A-119 require the federal government to use standards developed by voluntary consensus bodies in its regulatory and procurement activities, unless the use of such standards would be inconsistent with applicable law or otherwise impractical.

6. To the extent possible, existing standards should be leveraged, using international standards where applicable. Well-established standards that support patient safety in health IT already exist. Examples include those focused on quality management systems, risk management, safety, and software engineering developed by standards organizations such as the International Organization for Standardization (ISO).

7. The federal government should adopt the standards identified and agreed upon through this national approach and assure alignment of recognized standards across federal agencies to avoid areas of conflict or duplication.

8. Those who develop, implement, and use clinical software should voluntarily adhere to federally recognized standards identified and agreed upon through the national approach described above.

Leverage Conformity Assessment Tools

We concur that conformity assessment tools, such as product testing, certification, and accreditation can provide assurance that certain products, services, systems, or organizations meet specified standards or fulfill certain requirements. Attestation can also play a key role. We agree that these tools should be applied in a risk-based manner to distinguish high quality products, developers, vendors, and organizations from those that fail to meet a specified level of quality, safety, or performance. We further agree that non-governmental, independent programs should perform such conformity assessments. These concepts are consistent with the BPC report.

We also offer the following comments, drawing from the April 2014 letter developed by BPC, Health IT Now, and HIMSS and agreed upon by a diverse group of stakeholders.

1. Adherence to standards should be demonstrated through existing or new conformity tools, which can include but not be limited to accreditation, certification, and attestation facilitated by bodies recognized by the federal government.

2. Methods to demonstrate adherence must be flexible and reflect the continued evolution and complexity of health IT, continued research, and a changing evidence base. They should not be unduly burdensome or prescriptive.

3. The federal government should rely upon such conformity tools for its own regulatory processes related to health management software and should avoid duplicative and/or conflicting regulatory requirements.

Create an Environment of Learning and Continual Improvement

An effective oversight framework for health management software should be data driven. It should support and promote reporting, sharing, and analysis of patient safety events in a non-punitive environment that maintains confidentiality and enables learning and improvement.

We concur that the creation of an environment of learning and continual improvement is central to a health IT framework that protects patient safety and promotes innovation. We also concur that such a system should support the following, which are consistent with the BPC report.

- Identify, report, and respond to health IT-related adverse events and near misses;
- Aggregate and analyze events and near misses to identify patterns and trends;
- Support the development and adoption of interventions and mitigations, where appropriate; and
- Promote system-wide education and learning for stakeholders resulting in a system that is continually undergoing improvement.

In addition, we offer the following comments, drawn from an April 2014 letter developed by BPC, Health IT Now, and HIMSS and agreed upon by a diverse group of stakeholders.

1. **Leveraging Existing Authorities.** Rather than creating new, duplicative authorities, technical structures, and approaches, existing authorities, such as those contained in the *Patient Safety and Quality Improvement Act of 2005,* as well as related reporting, processes, and systems, should be leveraged.

2. **Integrated Reporting Structures.** Reporting structures should reflect the fact that health IT safety is part of a larger socio-technical system, with shared responsibility among developers, implementers, and users across the entire health IT lifecycle. Siloed reporting systems focused solely on health IT would result in duplicative reporting, unnecessary burden, and failure to capture many events.

3. **Requirements for Reporting.** When there are legal protections, developers, implementers, and users should participate in the reporting of health IT safety events, with requirements for reporting that cause death or serious harm. Such requirements already exist for many providers. This reporting can be accomplished through patient safety organizations, conformity assessment bodies, or other entities. Such reporting policies are not intended to limit or take the place of current provider reporting of patient safety issues directly to health IT vendors.

4. **Non-Punitive Environment That Encourages Reporting, Learning, and Improvement**. Creating a non-punitive environment will encourage reporting of all events, including hazards, unsafe conditions, and near misses, to support learning and improvement. As noted in the recent Institute of Medicine report on patient safety and health IT, in other countries and industries, reporting systems differ with respect to their design, but the majority employs reporting that is voluntary, confidential, and non-punitive. To encourage reporting and create a learning environment, the Department of Health and Human Services (HHS) should extend confidentiality protections currently provided to providers, to health IT developers and vendors to expand their participation in reporting and other patient safety-related activities.

   Aggregation, Analysis, and Dissemination to Support a Learning Health Care System. A system-wide approach, including the aggregation and analysis of reports which protect the confidentiality of patients, providers, products, and vendors across large populations, enables identification of underlying patterns and trends, as well as emerging risks. This also supports the development and implementation of interventions to mitigate risk and enables system-wide learning and improvement. The use of common formats and standards play a key role in effective analysis of aggregated data.

5. **Efficient and Non-Duplicative Processes.** Reporting efforts should take into account existing work flows, and the burden of reporting should be minimized. Federal agency policies associated with reporting should be clear, consistent, and non-duplicative both in language and enforcement. The federal government should recognize and leverage existing reporting processes, including those that reside in the private sector, to identify health IT-related events that cause death or serious harm with appropriate protections of privacy and confidentiality and avoid the creation of duplicative or conflicting reporting processes or systems.

Health IT Safety Center

We concur with the establishment of a Health IT Safety Center as outlined in the FDASIA report. We also agree that the Health IT Patient Safety Center should require strong governance and conduct activities that:

- Establish a broad and engaged stakeholder membership and leadership base;
- Focus on high-value issues (that are evidence-based) affecting the promotion of innovation and the protection of patient safety related to health IT;
- Build upon and improve the evidence-based foundation for health IT safety by analyzing the best available data and evidence and by identifying interventions and opportunities for improvement based on the data and evidence;
- Inform health IT safety priority goals and measures that align with broader patient safety goals and initiatives; and
- Provide education on health IT safety, including best practices regarding risks, mitigation strategies, usability, workflow, etc. to improve the commitment and capabilities of participant organizations to improve their health IT safety efforts and evaluate the effects of that education.

Thank you again for the opportunity to provide input on this draft report. We urge the Agencies to give thoughtful consideration to our comments as they progress toward a final strategy and set of recommendations for a risk-based framework for health IT.

We welcome the opportunity to discuss any specific questions you may have and look forward to continuing to work with the Agencies on this critical mission.

Sincerely,

Janet Marchibroda
Director, Health Innovation Initiative