BIPARTISAN POLICY CENTER

August 31, 2013

Jodi Daniel
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
Attention: FDASIA
200 Independence Avenue, S.W., Room 445-G
Washington, D.C. 20201

Dear Ms. Daniel,

The Bipartisan Policy Center is pleased to offer our comments in response to the May 30, 2013 Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology (IT).

These comments were based on the Bipartisan Policy Center report, An Oversight Framework for Assuring Patient Safety in Health Information Technology, released to the public on February 13, 2013.

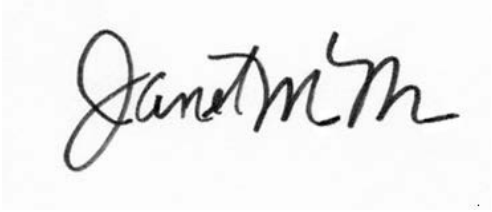
The BPC report contains principles and recommendations for an oversight framework for health IT that protects patient safety, is risk-based, promotes innovation, is flexible, leverages existing quality and patient safety-related systems and processes, avoids regulatory duplication, and has the support of experts and stakeholders across every sector of health care.

The principles and recommendations contained in the report were developed through a five-month collaborative effort involving more than 40 meetings and drawing upon the experiences and expertise of more than 100 experts and stakeholders representing clinicians, consumers, health plans, hospitals and other providers, mobile technology companies, patient safety organizations, research institutions, and technology companies.

We thank you for the opportunity to provide input to the administration's important work associated with FDASIA.

If you have any questions or require further information, please contact me via email at jmarchibroda@bipartisanpolicy.org or by phone at 202.379.1634.

Sincerely,



Janet M. Marchibroda
Director, Health Innovation Initiative

Attachment

# Formal Response to the 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

Bipartisan Policy Center
Health Innovation Initiative

August 31, 2013

BIPARTISAN POLICY CENTER

## ABOUT BPC

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole, and George Mitchell, Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation, and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policy making with strong, proactive advocacy and outreach.

## DISCLAIMER

This report is the product of the Bipartisan Policy Center's Health Project. The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center, its founders, or its board of directors.

# Table of Contents

# Executive Summary

This document includes the Bipartisan Policy Center's (BPC's) response to the FDASIA: Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology. BPC's response is based on a report it developed and released on February 13, 2012, An Oversight Framework for Assuring Patient Safety in Health Information Technology.

Through a collaborative five-month effort, BPC conducted research and engaged more than 100 experts and stakeholders representing clinicians, consumers, health plans, hospitals and other providers, mobile technology companies, patient safety organizations, research institutions, and technology companies, holding more than 40 meetings, to develop a set of principles and recommendations for the key elements of an oversight framework for health information technology (IT), that are contained in the BPC Report. A list of the organizations that contributed their time and expertise to this effort are summarized in the "Acknowledgements" section on page 34.

The principles and recommendations included in the Report—and summarized below—call for a framework that protects patient safety, is risk-based, promotes innovation, is flexible, leverages existing quality and patient safety-related systems and processes, avoids regulatory duplication, and has the support of experts and stakeholders across every sector of health care.

BPC encourages the administration to take into consideration the principles and recommendations included in An Oversight Framework for Assuring Patient Safety in Health Information Technology as it develops a strategy and recommendations for an appropriate risk-based regulatory framework pertaining to health IT, including mobile medical applications, in response to the Food and Drug Administration and Innovation Act of 2012 (FDASIA).

## Principles for an Oversight Framework for Health IT

The following set of principles, contained in the BPC Report, should guide the federal government's strategy and recommendations for a regulatory framework for health IT.

1. Any oversight framework for safety should recognize and support the important role that health IT plays in improving the quality, safety, and cost-effectiveness of care, as well as the patient's experience of care.
2. Assuring patient safety, along with enabling positive patient outcomes, is a shared responsibility that must involve the entire health care system.

3. Any framework for patient safety in health IT should be risk-based, flexible, and not stifle innovation.
4. Existing safety and quality-related processes, systems, and standards should be leveraged for patient safety in health IT.
5. Reporting of patient safety events related to health IT is essential; a non-punitive environment should be established to encourage reporting, learning, and improvement.

## Key Elements of an Oversight Framework for Health IT

As outlined in the BPC Report, clinical software should be subject to an oversight framework that includes four key elements:

1. Agreement on recognized standards and guidelines for assuring patient safety in the development, implementation, and use of health IT.
2. Support for the implementation of standards and guidelines as well as development and dissemination of best practices through education, training, and technical assistance.
3. Developer, implementer, and user participation in patient safety activities, leveraging patient safety organizations (PSOs), including reporting, analysis, and response.
4. Creation of a learning environment through the aggregation and analysis of data to identify and monitor trends, mitigate future risk, and facilitate learning and improvement.

# Background

This document includes the Bipartisan Policy Center's (BPC's) response to the FDASIA: Request for Comments on the Development of a Risk-Based Regulatory Framework and Strategy for Health Information Technology (Request for Comments), that was published on May 30, 2013 in the Federal Register. This response is based on a report released by BPC earlier this year, An Oversight Framework for Assuring Patient Safety in Health Information Technology (BPC Report).

In September 2012, BPC launched a significant effort in response to a key component of The Food and Drug Administration Safety and Innovation Act of 2012 (FDASIA), which calls for the Secretary of the Department of Health and Human Services (HHS) to post—within 18 months (or by January 2014)—a report that contains a proposed strategy and recommendations 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.

Through a collaborative effort, BPC both conducted research and engaged a wide range of stakeholders and experts to develop a set of principles and recommendations for an oversight framework for health IT that protects patient safety, is risk-based, promotes innovation, is flexible, leverages existing quality and patient safety–related systems and processes, avoids regulatory duplication, and has the support of experts and stakeholders across every sector of health care.

The principles and recommendations contained in the BPC Report were developed through a five-month, collaborative effort involving more than 40 meetings and drawing upon the expertise and experiences of more than 100 experts in patient safety and IT and leaders representing clinicians, consumers, health plans, hospitals and other providers, mobile technology organizations, patient safety organizations, research institutions, and technology companies, including those that develop electronic health records. A list of the organizations that contributed their time and expertise to this effort are summarized in the "Acknowledgements" section on page 34.

The BPC Report was released on February 13, 2013 at a public event held at BPC and featuring numerous public and private sector leaders.

In its Request for Comments, HHS asked for public input on three topics: taxonomy, risk and innovation, and regulation. The questions outlined in the Request for Comments, are summarized below.

1. Taxonomy
    a. What types of health IT should be addressed by the report developed by FDA, ONC, and FCC?
2. Risk and Innovation
    a. What are the risks to patient safety posed by health IT and what is the likelihood of these risks?
    b. What factors or approaches could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety?
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.
    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?

BPC addresses each of the questions posed by the Request for Comments, below. Following the release of the BPC Report, the BPC Health Innovation Initiative has continued to study and engage experts and stakeholders in dialogue regarding key aspects of the report. To date, BPC has focused on more fully defining health IT functions to facilitate the development of criteria and an approach for determining the level and type of oversight to be applied. BPC's work-in-progress on this effort is included in this paper.

# Taxonomy

The Request for Comments asks about the types of health IT that should be addressed by the report developed by FDA, ONC, and FCC.

The report developed by FDA, ONC, and FCC should be comprehensive, addressing all types of health IT, including mobile medical applications, to provide clarity and guidance regarding the following for different types of health IT: (1) whether or not additional oversight is required; (2) the types of additional oversight that will be applied, if applicable; and (3) the organizations (e.g., the federal agencies or types of private sector organizations) that are expected to carry out such oversight.

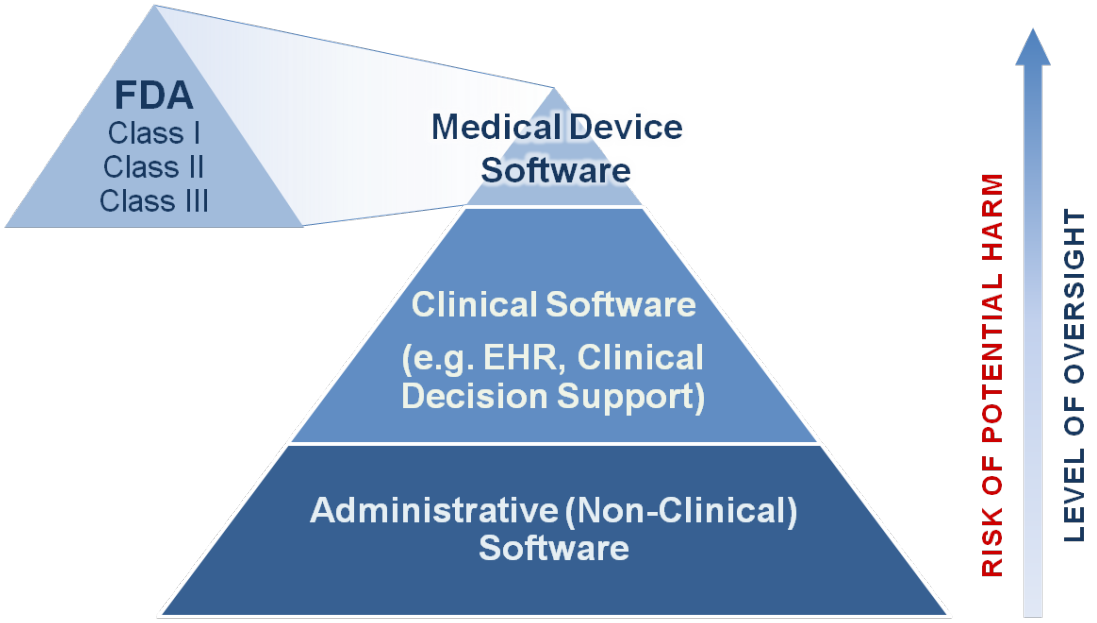
Health IT includes software and its hardware and process dependencies used in the health sector that can have an impact on the health and health care of a subject(s) of care. Hardware and software dependencies include network and end user equipment, availability of power the loss of which can cause unexpected downtime, and process elements such as use, configuration and customization.

Health IT includes a broad range of products, including but not limited to: electronic health records, patient engagement tools, health information exchange software, administrative tools such as those that facilitate admissions, billing, and other related transactions, decision support, and the capacity for clinicians and patients to see the patient's clinical progress and data more easily. A health IT oversight framework should also include consideration of system interfaces and infrastructure that enable interoperability and electronic information sharing, between health IT products and across organizational boundaries.

Health IT can deliver information to users from numerous platforms—servers, personal computers, and a large variety of mobile devices. It would be difficult—if not impossible—to predict what new platforms will evolve in the future. An oversight framework should be "platform-agnostic".

The BPC Report recommends that health IT be assigned to one of three categories based upon the level of risk of patient harm (illustrated in Figure 1 below): (1) medical device software, which should continued to be regulated by FDA as a medical device; (2) clinical software, which should be subject to a new oversight framework outlined in more detail below and in the BPC report; and (3) administrative or non-clinical software, which should not be subject to additional oversight, given its level of risk.

**Figure 1. A Risk-Based Oversight Framework for Health IT**




Following the release of the February 2013 report, BPC continued to engage experts and stakeholders in dialogue regarding methods and an approach for categorizing the different types of health IT for the purpose of determining the level and types of oversight to be applied. As part of this process, health IT functions were identified and assigned to categories of risk and oversight included in the BPC oversight framework. Work in progress can be found in this paper.

# Risk and Innovation

## Health IT and Patient Safety

The RFC asks about the risks to patient safety posed by health IT and the likelihood of these risks.

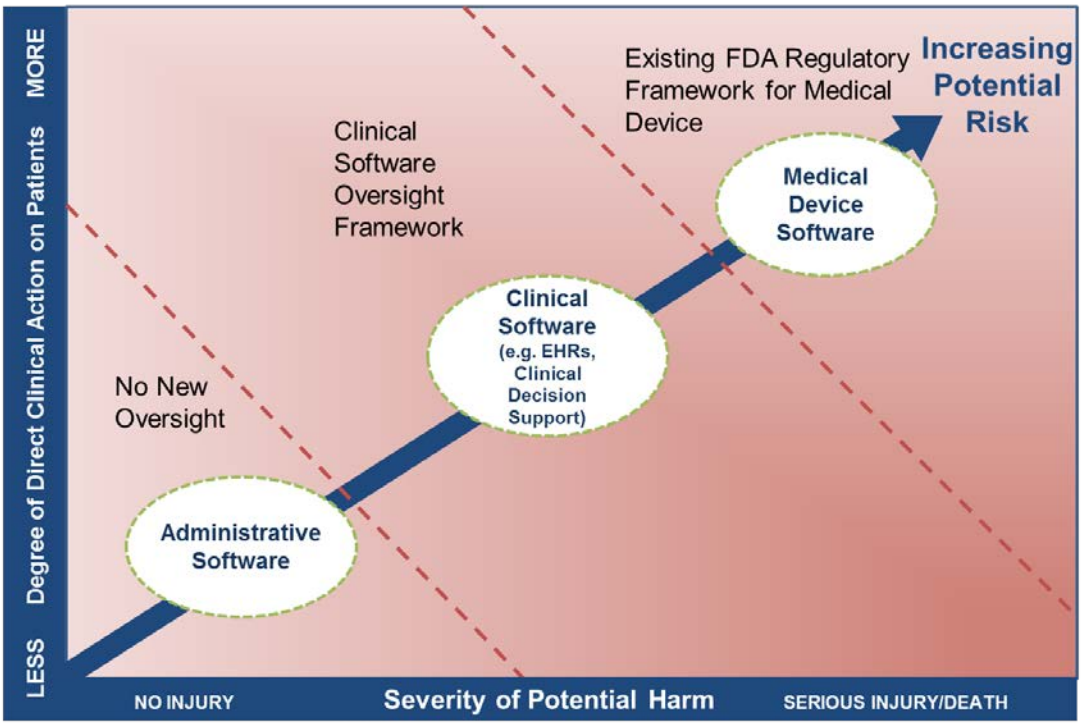
As noted in the BPC report, more than ten years ago, the Institute of Medicine (IOM) released two landmark reports that catalyzed efforts to improve patient safety in U.S. health care.[1,2] Both reports highlighted the critical role that health IT plays in improving the quality and safety of care. Several studies have shown that health IT, if effectively designed and implemented, has a positive impact on patient safety, the efficiency and effectiveness of care, and patient and provider satisfaction.[3]

The widespread adoption of health IT largely stems from recognition of the important role that it plays in improving health care quality and safety. Rapidly emerging delivery system and payment models designed to improve quality, reduce costs, and improve the patient's experience of care require a strong IT foundation to be successful.

However, there are also instances in which it has the potential to create harm if not effectively developed, implemented, or used. Current data, however, suggests that the level of overall risk (based on incidence and prevalence) is quite low. A recent IOM report indicated that health information systems were involved in less than 1 percent of reported errors in health care settings.[4] A recently published advisory notice from the Pennsylvania Patient Safety Authority noted that only 3,900 of 1.7 million reports were found to involve health IT.[5]

The BPC Report calls for an oversight framework based on risk and outlines key factors to be considered in the evaluation of risk, illustrated in Figure 2 below. Such factors include the potential for patient harm, the severity or extent of harm, and the extent to which the software directly interacts with patients (which can be otherwise described as the level of opportunity for clinical intervention).

**Figure 2: Factors That Determine the Level of Oversight**




The RFC asks about the factors or approaches that could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety.

The BPC Report recommended a set of principles that should guide the federal government's development of an oversight framework for IT. These principles, along with background associated with each principle—drawn directly from the BPC Report—are summarized below.

## Principles for an Oversight Framework for Health IT

### 1. ANY FRAMEWORK FOR SAFETY SHOULD RECOGNIZE AND SUPPORT THE IMPORTANT ROLE THAT HEALTH IT PLAYS IN IMPROVING THE QUALITY, SAFETY, AND COST-EFFECTIVENESS OF CARE, AS WELL AS THE PATIENT'S EXPERIENCE OF CARE.

Research shows that health IT has a positive impact on the quality, safety, and cost-effectiveness of health care.[6] Health IT plays a foundational role in the broadly supported national imperative to improve health and health care for all Americans.

While the widespread adoption of health IT largely stems from recognition of the important role that it plays in improving health care quality and safety, there are also instances in which it can create harm if not effectively developed, implemented, or used.

Because of the significant role that health IT plays in improving the quality, safety, and cost-effectiveness of care, as well as the patient's experience of care, any framework for safety should both recognize and support innovation in and adoption of health IT.

## 2. ASSURING PATIENT SAFETY, ALONG WITH ENABLING POSITIVE PATIENT OUTCOMES, IS A SHARED RESPONSIBILITY THAT MUST INVOLVE THE ENTIRE HEALTH CARE SYSTEM.

Assuring patient safety in health IT is a shared responsibility among the many stakeholders within the health care ecosystem. As noted in the recent IOM report, safety is part of a larger sociotechnical system that takes into account not just the software, but also how it is used.[7] This larger system includes technology, people, processes, organizations, and the external environment.[8]

The level of safety in health IT depends on how the technology is designed, customized, implemented, used, maintained, and incorporated into clinical workflows. The quality of data, the interoperability of IT systems, and the appropriateness of clinical interventions also have an impact on health IT safety. Additionally, education, training, and proficiency of users can play a critical role. Finally, health IT supports—but does not replace—the judgment of clinicians.

Any oversight framework for safety in health IT should have strong support from and involvement of all stakeholders, including patients.

## 3. ANY FRAMEWORK FOR PATIENT SAFETY IN HEALTH IT SHOULD BE RISK-BASED, FLEXIBLE, AND SHOULD NOT STIFLE INNOVATION.

The scale and scope of oversight requirements intended to ensure patient safety in health IT should be correlated to the potential risk of harm to patients.

Health care is a continually evolving ecosystem that is now undergoing considerable change. Health IT plays a foundational role for rapidly emerging new models of delivery and payment that promise to improve the quality, safety, and cost-effectiveness of care, such as accountable care arrangements and the patient-centered medical home.

Health IT must evolve to support rapidly emerging changes in the health care system and must continually be upgraded and/or customized to address the ever-changing needs of those who deliver, manage, pay for, and receive care. Innovation is needed to continually drive improvements in the cost, quality, and patient experience of care.

Any framework for safety in health IT must be flexible and promote—not stifle—the innovation needed to drive further improvements in health and health care. Current regulatory frameworks that are oriented toward turnkey devices that change infrequently and are often not customized based on the needs of the user, do not align well with the current and anticipated nature of health IT.

## 4. EXISTING SAFETY AND QUALITY-RELATED PROCESSES, SYSTEMS, AND STANDARDS SHOULD BE LEVERAGED FOR PATIENT SAFETY IN HEALTH IT.

Policies, processes, and systems associated with assuring safety in health IT should be aligned with and integrated into well-established patient safety and quality programs, including those that involve accreditation, certification, and reporting.

Quality management and safety principles, processes, and standards, which are well-established and common to other industries, should also be leveraged for assuring patient safety in health IT.

Health IT is an essential component of a comprehensive approach to improving patient outcomes and assuring the quality, safety, and efficiency of health care. Any oversight framework for health IT should align with and leverage existing processes, systems, and standards in health care, and should discourage or prevent duplicative or inconsistent requirements.

## 5. REPORTING OF PATIENT SAFETY EVENTS RELATED TO HEALTH IT IS ESSENTIAL; A NON-PUNITIVE ENVIRONMENT SHOULD BE ESTABLISHED TO ENCOURAGE REPORTING, LEARNING, AND IMPROVEMENT.

Any framework for patient safety in health IT 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.

Reporting of patient safety events by users, developers, implementers, and patients is essential to both gaining an understanding of the nature and magnitude of health IT–related safety events and developing and implementing strategies to address risks. Aggregation and analysis of events and timely feedback to developers, implementers, and users are also crucial, so that necessary changes can be made to address identified issues and to mitigate future risk.

Existing reporting processes and bodies, such as those created by the Patient Safety and Quality Improvement Act, should be leveraged. Reporting efforts should be coordinated. They should take into account existing work flows, and the burden of reporting should be minimized. The use of consistent formats for reporting should be encouraged so that data can be easily aggregated and analyzed to support learning and improvement.

Reporting policies should encourage reporting for learning and improvement. As noted in the recent IOM report, “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.”[9] Lessons learned from such other approaches should be integrated into any oversight framework for health IT.

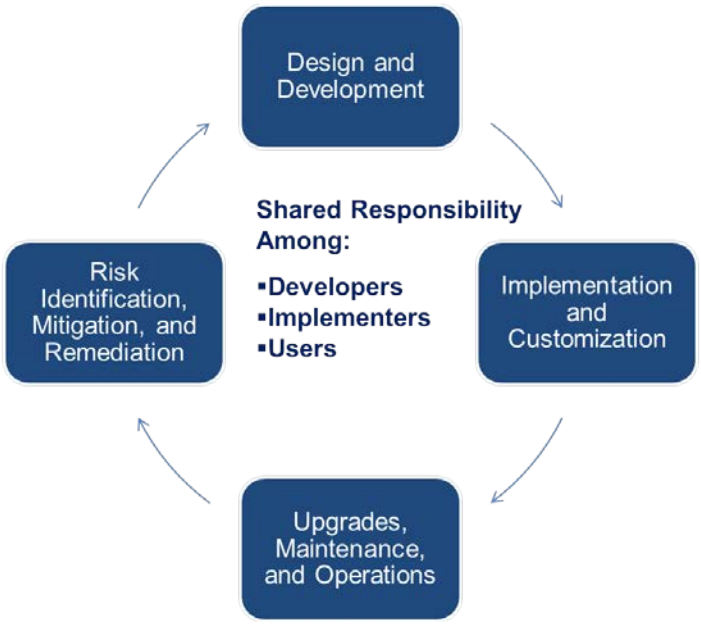
# Key Considerations for Oversight

The BPC report offers several considerations for an oversight framework for health IT, which are summarized below.

First, the safety of health IT relies not only on how it is designed and developed, but also on how it is customized, implemented, and used. As illustrated in Figure 3 below, safety in health IT, is a shared responsibility among developers, implementers, and users across the various stages of the health IT life cycle. The health IT life cycle stages include (1) design and development; (2) implementation and customization; (3) upgrades, maintenance, and operations; and (4) risk mitigation and remediation.

"Developers" are defined as those who develop software for use in health care and can include commercial IT companies, academic institutions, and health care organizations. "Implementers" are defined as those who implement software in the health care setting, and can include the IT and medical informatics departments of provider institutions, consultants, commercial health IT companies, and, in some cases, clinicians and practice management staff. "Users" are defined as those who actually use the software.

**Figure 3: Stages of the Health IT Life Cycle**



As noted in the BPC Report, other factors that impact the level of patient safety in the use of health IT include the quality of data that resides in health IT systems, the level of interoperability and exchange of information across systems, the integration of the software into clinical work flows, and the appropriateness of clinical interventions.

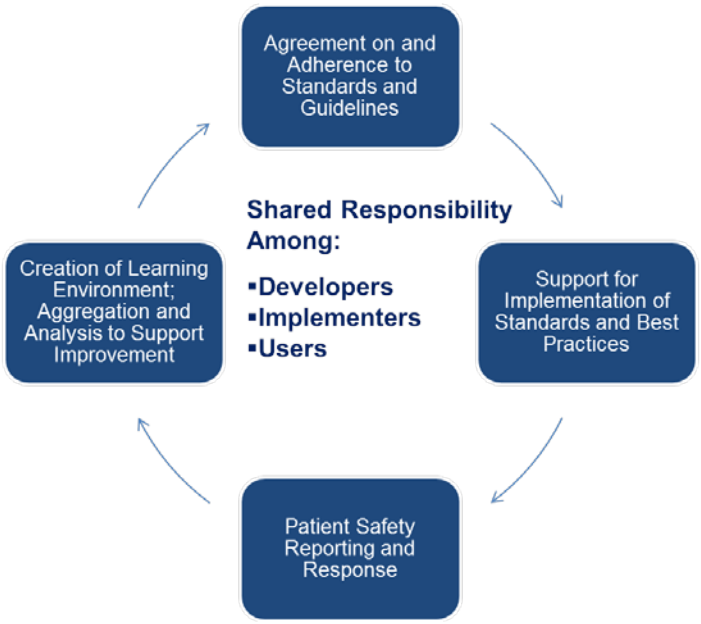
For the most part, health IT is designed to inform—not take the place of—clinical decision-making. Health IT supports but does not replace the judgment of clinicians. The ability to mitigate harmful conditions has an impact on risk.

Health IT is constantly being upgraded and modified to reflect new evidence and clinical interventions, changing work flows, and new requirements now rapidly emerging from public- and private-sector agencies. A regulatory framework should be flexible enough to accommodate constantly evolving systems, the changes for which are implemented by developers, users, and implementers.

## Key Elements of Oversight for "Clinical Software" (Middle Tier in the Framework)

The BPC report outlines four key elements of oversight for clinical software, illustrated in Figure 4 below. "Clinical software" represents the middle tier of the Oversight Framework illustrated in Figure 1. Addressing these four elements is a shared responsibility among developers, implementers, and users of clinical software.

**Figure 4. Oversight Framework for Clinical Software**



The four key elements are explored in more detail below, drawing from the BPC Report.

## 1. AGREEMENT ON AND ADHERENCE TO RECOGNIZED STANDARDS AND GUIDELINES FOR ASSURING PATIENT SAFETY

As noted in the BPC Report, one of the key components of an oversight framework for clinical software is agreement on and adherence to standards and guidelines for assuring patient safety in the development, implementation, and ongoing use of health IT.

Because assurance of safety in health IT is a shared responsibility that is dependent on how it is developed, implemented, and used, standards and guidelines for assuring patient safety should focus on harmonized processes across the health IT life cycle—as opposed to technical requirements that are limited to specific product functionality. A process and life cycle approach inherently leads to higher product safety as it enables the delivery of defined and consistent outcomes.

As noted in the IOM report on patient safety and health IT, experiences from other industries suggest the best approach to proactively creating highly reliable products is not to certify each individual product but rather, to make sure organizations have adopted quality-management principles and processes in the design and development of products.[10]

Developers, implementers, users, and patients, along with patient safety and health IT experts and government, should both inform and play a significant role in the development and continued evolution of such standards and guidelines.

Independent "voluntary consensus bodies"—defined by OMB Circular A-119 as those that exhibit the attributes of openness, balance of interest, due process, an appeals process, and consensus—are in the best position to facilitate agreement among health care stakeholders on a recognized set of standards and guidelines for patient safety in health IT.[11] Under the National Technology Transfer and Advancement Act of 1995 and OMB Circular A-119, the federal government is required 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.[12,13]

Well-established international standards that enable patient safety already exist and are developed under the auspices of the International Organization for Standardization (ISO). BPC has identified several process standards applicable to HIT, summarized in Figure 5 below.

The complete range of existing standards and guidelines should be reviewed for applicability to health IT patient safety goals, gaps should be identified and modified, and new standards should be developed as needed. Funding of research in areas where gaps are identified will be needed.

Such standards and guidelines must continually evolve to address changing requirements and the identification of new issues that need focus. Standard and guideline development processes should be tightly linked to and informed by the analysis of aggregated reports from across the health care system, to facilitate learning and improvement.

**Figure 5: Existing Standards to be Explored for Health IT Oversight**

- ISO 9000 series on Quality Management Systems
- ISO/IEC JTC1 Series of Software and Systems Engineering Standards
- ISO/IEC 2101 Risk Management – Risk Assessment Techniques
- ISO/IEC 24748 Systems and Software Engineering Life Cycle Management
- ISO/IEC 15504 Information Technology Process Assessment
- ISO/IEC 15206 Systems and Software Engineering Systems and Software Assurance Series
- AAMI TIR 362007 Validation of Software for Regulated Purposes
- ISO 27799 Health Informatics Information Security Management in Health Using ISO/IEC 27002
- ISO 2000 Series Information Technology Service Management
- IEC 62304 Medical Device Software Lifecycle Processes
- ISO 13485 Medical Device Quality Management Systems
- ANSI/AAMI SW87 Application of Quality Management Systems Concepts to Medical Device Data Systems
- ISO 14971 Medical Device Application of Risk Management to Medical Devices
- IEC 8001-1 Application of Risk Management for IT Networks Incorporating Medical Devices
- AAMI TIR45 Guidance on Use of Agile Practices in Development of Medical Device Software
- ISO TR 27809 Health Informatics Measures for Ensuring Patient Safety of Health Software
- ISO TS 25238 Health Informatics Classification of Safety Risks from Health Software

Developers and software implementers that are not a part of provider organizations should demonstrate adherence to recognized and agreed-upon standards and guidelines by undergoing accreditation administered through independent, recognized bodies that operate in the private sector.

BPC is in the process of exploring the governance and attributes of such bodies, learning from existing experiences both inside and outside of health care. BPC also plans to explore whether any additional legislative or regulatory authority is needed to support the recognition of the work of such bodies by federal agencies for purposes of oversight.

As part of this process, BPC also plans to examine in further detail—with multi-stakeholder input--the appropriate balance and combination of accreditation, certification, and attestation processes that will help to assure confidence and compliance with agreed-upon patient safety-related standards.

The BPC Report also notes that existing, independent provider accreditation bodies should also reference and support recognized standards and guidelines for software implementation and use.

## 2. SUPPORT FOR IMPLEMENTATION OF STANDARDS AND GUIDELINES; DEVELOPMENT AND DISSEMINATION OF BEST PRACTICES FOR DEVELOPERS, IMPLEMENTERS, AND USERS

As noted in the BPC Report, widespread dissemination of and support for the implementation of standards, guidelines, and best practices for assuring safety in the development, implementation, and use of clinical software is crucial. This can take the form of education, training, and implementation support services offered by organizations with expertise in this area, as well as those who work with software vendors, clinicians, hospitals, and other providers.

More dialogue and collaboration on best practices for assuring safety in the use of health IT is needed among those who develop, implement, and use software in health care. Fear of liability, punitive or regulatory action, and negative press, combined with some lack of trust, all serve as barriers to dialogue among clinicians, hospitals, and technology developers about the actions that can be taken to continually improve patient safety in health IT–enabled care.

Developers, implementers, users, health IT and patient safety experts, and PSOs should collaborate on the development and dissemination of strategies and best practices for assuring patient safety throughout the health IT life cycle. The phases of the life cycle include the design and development; implementation and customization; upgrade, maintenance, and operations; and risk identification, mitigation, and remediation phases of the health IT life cycle. Such strategies and best practices should align with recognized standards and guidelines. This will require significant investment of resources in research, collaboration, and dissemination.

## 3. PARTICIPATION IN PATIENT SAFETY ACTIVITIES INCLUDING REPORTING, ANALYSIS, AND RESPONSE

As noted in the BPC Report, reporting, analysis, and development and execution of corrective actions for individual patient safety events are critical components of an oversight framework for patient safety in health IT. Four issues associated with reporting, analysis, and response—summarized below--were explored in the BPC Report.

### Leveraging Existing Patient-Safety Related Authorities, Organizations, and Processes

Congress passed the Patient Safety and Quality Improvement Act of 2005 (the Patient Safety Act), to encourage health care providers to voluntarily report information on patient safety events and to facilitate the development and adoption of interventions and solutions to improve patient safety.

Rather than establish new authorities or structures for reporting and analysis of patient safety events specific to health IT, those brought about by the Patient Safety Act—including patient safety organizations (PSOs)—should be leveraged to support reporting and analysis of health IT–related patient safety events.

As indicated in the BPC Report, creating a safety reporting silo that only focuses on health IT would be duplicative, increase unnecessary burden, and also result in the failure to capture many relevant events. Patient safety events associated with health IT are often not identified as such until analysis has been performed by the PSO. Many patient safety problems that have health IT dimensions are characterized by the providers that report them in other ways, such as medication errors, patient identification errors, erroneous laboratory or radiology results, or documentation or communication errors. For example, 43 percent of the device and health IT events in one large PSO database were submitted in a non-health-IT-related category.[14]

### Enabling Developers to Participate in Patient Safety Activities

As noted in the BPC Report, many providers voluntarily report patient safety events to PSOs. In addition, a majority of states have mandatory hospital and other health care provider reporting requirements related to events that cause death or serious harm.[15] The Joint Commission, through its accreditation process, reviews hospitals' activities in response to sentinel events (which are unexpected occurrences involving death or serious injury) and encourages—but does not require—the reporting of such events to Joint Commission's Sentinel Event Database.[16]

PSOs work with clinicians, hospitals, and other providers to analyze and understand the root cause of patient safety events, provide feedback, and develop and disseminate recommendations designed to improve quality and safety. In the case of patient safety events that involve health IT, developers and implementers of software also play a critical role in gaining an understanding of root cause and other contributing factors.

Unless developers have a direct relationship with a PSO, they are not able to participate with the PSO in analyzing, identifying the root causes of, and developing corrective actions for health IT–related patient safety events, because sharing a report with them would break statutory confidentiality protections. Under the Patient Safety Act, developers may have a relationship with a PSO either by becoming a PSO, entering into a joint venture with the PSO, or serving under contract to the PSO, which permits them to participate in patient safety activities.

Because health IT safety is a shared responsibility, health IT developers must have the ability to participate with PSOs, clinicians, hospitals, and other providers in patient safety activities to improve the safety and quality of health IT–enabled care without breaking statutory confidentiality protections for providers.

While clinicians, hospitals, and other providers are often in the best position to identify and report patient safety events associated with health IT, there may be situations in which developers or implementers of software are made aware of events associated with use of health IT products through communications with their clients.

Because assuring patient safety in health IT is a shared responsibility, developers—like providers--should report patient safety events to PSOs, as appropriate, with expanded protections and requirements for reporting of events that cause death or serious harm.

The current law should be extended to provide confidentiality protections to health IT developers to permit them to report patient safety events, view PSO-protected information, receive and analyze event reports, create and receive quality-improvement recommendations from the PSO, and work with the providers to develop strategies for improvement.

Like providers, such protections would not exempt developers from lawsuits. Information in the patient's medical record concerning the underlying facts involving any health IT is not protected under the Patient Safety Act and remains available to plaintiffs. Therefore, extending the protections to develop a culture of safety would not limit a developer's potential liability if one of its products directly causes harm to a patient. Additionally, health IT developers and their products must also comply with existing federal or state consumer protection laws, as well as federal and state privacy and security laws and regulations. In summary, expanded protections for developers would not affect laws that are intended to protect patients and consumers.

The Agency for Healthcare Research and Quality (AHRQ) should explore options for enabling developers to participate in patient safety activities with protections. Such participation would include reporting, review and analysis of patient safety events that are health IT-related, creation and receipt of quality improvement recommendations from the PSO associated with a specific event, and dialogue with the PSO and provider regarding corrective actions that can be taken to mitigate further risk.

### Removing Barriers to Reporting Among Clinicians and Other Providers

As noted in the BPC Report, one of the primary barriers to reporting among clinicians, hospitals, and other providers is the burden of reporting and its impact on current work flows. The administration and management of reporting takes considerable time and resources. Reporting efforts should be designed to minimize the burden of reporting. To the extent feasible and possible, reporting should be embedded into current work flows and health IT systems.

Another key barrier is the lack of awareness or understanding of the confidentiality protections under the Patient Safety Act. Awareness-building and education programs designed to explain and clarify both the benefits of reporting and the confidentiality protections that are in place can support expanded reporting by clinicians, as well as other providers. Organizations representing PSOs, developers, clinicians, hospitals, and other providers should take steps to encourage reporting of patient safety events—including those related to health IT. This can be accomplished by raising awareness of the benefits of reporting and clarifying the confidentiality protections in place to support such reporting. Expanded reporting will further the ability to learn more about the nature and prevalence of risk, enable the development of strategies and best practices to address areas of risk, and facilitate improvement in the quality and safety of health care.

Other barriers to patient safety reporting cited by clinicians include fear of breaching confidentiality provisions of contracts with their health IT vendors and, in some cases, perceived institutional barriers to reporting.

Raising awareness among clinicians and other providers by health IT vendors regarding the permissibility of reporting patient safety events to their PSOs under existing contracts, and further clarifying such language in future contracts, can help to allay such fears among clinicians and other providers. To address the perceptions of some clinicians that patient safety reporting might breach the confidentiality provisions of contracts with their health IT vendors, developers should raise awareness among their clients that reporting of patient safety events to their PSOs is indeed permissible under their existing contracts. In cases where there is lack of clarity, developers should work to clarify such language in future contracts to help allay fears among those clinicians and other providers who perceive contractual language to be a barrier.

Increasing awareness of the importance of and policies associated with patient safety reporting within institutions can also reduce clinician-perceived barriers to reporting.

### Expanding PSO Capabilities Associated with Health IT-Related Patient Safety Events

While there is a great deal of literature on improving patient safety generally in health care, relatively little is known or has been published about the nature and prevalence of patient safety events associated with health IT development and use.

The development of standards, guidelines, and best practices for reporting and analysis of reported events, development of corrective action plans, aggregation and analysis of large data sets, and development of strategies to mitigate future risk for health IT–related patient safety events—is needed. Such development must necessarily occur with significant involvement of developers, implementers, users, and patient safety and health IT experts.

## 4. CREATION OF A LEARNING ENVIRONMENT FOR SAFETY IN HEALTH IT

As noted in the BPC Report, reporting and responding to individual events is a critical means to enhance safety, but it is not enough. Aggregating and analyzing reports across large populations enables a more rapid identification of underlying patterns and trends as well as emerging risks and the causes of those risks. Aggregation and analysis of patient safety data also supports the development and implementation of interventions to mitigate risk and enable system-wide learning and improvement.

Regardless of the mechanisms used, appropriate governance, policies, protections, and capabilities will need to be established for entities that choose to aggregate large sets of patient safety data to garner trust, assure confidentiality, provide ease of use, minimize burden, and deliver value to participants—all of which will be required to promote significant participation and long-term sustainability.

Developers, implementers, users, PSOs, patient safety and health IT experts, and consumers should collaborate on the development of key attributes and requirements associated with the aggregation and analysis of non-identified patient safety event data to facilitate learning and to assure patient safety in the use of health IT. Such attributes and requirements will inform PSOs that wish to provide services associated with patient safety in health IT and help them gain the participation and support of developers, implementers, and users who wish to participate in aggregated reporting efforts designed to promote safety in health IT.

The use of standardized formats for reporting will significantly improve the ability for data to be aggregated and analyzed to support system-wide response and improvement.

Recognizing the importance of using standard formats for the reporting of patient safety events to enable aggregation, analysis, and identification of interventions that mitigate risk and support improvement; developers, implementers, and users who report patient safety events should be encouraged to utilize standardized formats.

Developers, implementers, users, and PSOs that report patient safety events should utilize standardized formats for such reporting—including those related to health IT.

# Regulations

As noted previously, the BPC Report recommends a new oversight framework for health IT that assigns health IT to one of three categories, based upon the level of risk of patient harm: (1) medical device software, which should continued to be regulated by FDA as a medical device; (2) clinical software, which should be subject to a new oversight framework outlined in detail both in this paper and within the BPC report; and (3) administrative or non-clinical software, which should not be subject to additional oversight, given its level of risk.

The Request for Comments asks if there are current areas of regulatory overlap among FDA, ONC, and/or FCC and if so, asks for a description. It also asks for actions that should be taken to minimize or avoid any overlap.

Health care organizations are highly regulated by states, the federal government including the Centers for Medicare and Medicaid Services, the Federal Communications Commission, Food and Drug Administration, and the Office of the National Coordinator for Health IT, and several federally recognized bodies such as the Joint Commission, the National Committee for Quality Assurance, and several health IT certification bodies. Each of these entities has requirements related to health IT.

The development of a risk-based regulatory framework and strategy for health IT called for by FDASIA offers an opportunity for FDA, ONC, and the FCC to conduct a careful review of all existing regulatory efforts that pertain to this work, and seek to minimize duplicative or conflicting regulations.

The administration should develop a comprehensive, risk-based regulatory framework that clearly defines and widely communicates how health IT with differing levels of risk will be regulated: by whom, how, etc. Such oversight should not be duplicative.

# Insights on FDASIA Workgroup Draft Recommendations

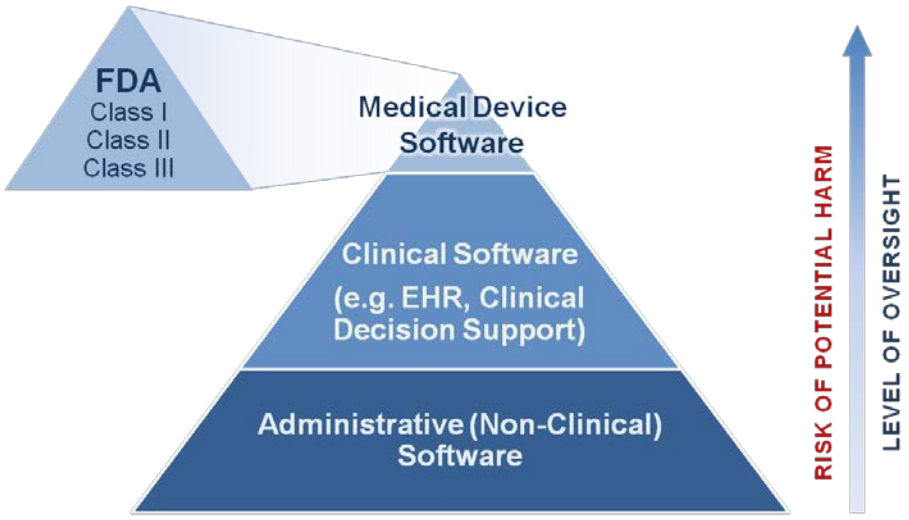
The FDASIA Workgroup was established by HHS in April 2013 to provide input into the development of recommendations for a risk-based regulatory framework for health IT, including mobile medical applications. It held its final meeting on August 13, 2013, in preparation for the submission of its final recommendations September 4, 2013 to the Health IT Policy Committee—a federal advisory committee established under HITECH in 2009.

The FDASIA workgroup's latest report draft was posted for public review on August 13, 2013. The following summarizes insights on and reactions to this draft report.

1. As written, the FDASIA Workgroup's draft recommendations for a regulatory framework for health IT, including mobile medical applications, are not clear. While some slides provide recommendations on the principles and attributes of a new oversight framework (which are in alignment with several aspects of the BPC oversight framework), others indicate that health IT should be regulated under an FDA medical device regulation regime.

   The BPC Report An Oversight Framework for Assuring Patient Safety in Health Information Technology, recommends a comprehensive oversight framework for health IT that assigns health IT to categories based upon the level of risk and applies different types of oversight based upon the level of risk.

   As illustrated below, BPC recommends that health IT be assigned to one of three categories, including (1) medical device software, which should continue to be regulated by the FDA as a medical device; (2) clinical software, which should be subject to a new oversight framework outlined in more detail above and in the BPC report; and (3) administrative or non-clinical software, which should not be subject to additional oversight, given its level of risk.




The Workgroup draft report does indicate that substantial additional regulation of health IT beyond what is currently in place is not warranted, with the exception of medical device data systems (MDDS), medical device accessories, certain forms of high risk clinical decision support, and higher risk software use cases, with which we agree.

2. The FDASIA Workgroup findings and recommendations should recognize the importance of shared responsibility, one of the primary principles outlined in the BPC Report.

   According to the BPC Report, assuring patient safety in health IT is a shared responsibility among the many stakeholders within the health care ecosystem. As noted in the recent IOM report, safety is part of a larger sociotechnical system that takes into account not just the software, but also how it is used.[17] This larger system includes technology, people, processes, organizations, and the external environment.[18]

   The level of safety in health IT depends on how the technology is designed, customized, implemented, used, maintained, and incorporated into clinical workflows. Attention should be paid to all aspects of the health IT life cycle, including design and development; implementation and customization; upgrades, maintenance, and operations; and risk mitigation and remediation.

   Addressing only the pre-market or development phase of the life cycle will not facilitate the rapid identification and investigation of, and response to adverse events caused by the development, implementation, and use of health IT. Utilization of siloed approach will not adequately achieve the primary goal of a comprehensive regulatory framework—which is to improve patient safety as it relates to health IT.

3. BPC commends the Workgroup for its significant work associated with the evaluation of risk, including the identification of risk factors, such as severity of injury, likelihood of hazardous situation arising, ability to mitigate harmful conditions, and transparency of software operations and data.

   We recommend that the Workgroup clarify and illustrate in its examples of how risk factors should be applied that all risk factors do not carry the same weighting. As currently written, the draft examples have the potential of being misleading.

   Furthermore, as noted in this paper, risk factors should be applied to health IT functionality—not health IT products. Products—such as electronic health records, personal health records, and clinical decision support software are not "one-size-fits-all". Their functionalities vary considerably and the risk associated with such functionalities, also vary considerably.

4. Several of the FDASIA Workgroup draft recommendations associated with a new oversight framework align with the principles and recommendations included in the BPC report, including:

   - Key principles of oversight that include a focus on shared learning, maximization of transparency, a non-punitive approach, identification of appropriate levels of accountability, and minimization of burden.
   - A new framework that fosters both national accountability using national and international standards and a learning environment that encourages multiple solutions, continuous innovation, measurement of results, and participation.
   - Better post-market surveillance of health IT, using a collaborative process with stakeholder participation.

# Health IT Functions and Characterization of Risk

The Bipartisan Policy Center is in the process of developing recommendations for a set of evaluation criteria, methods, and processes that can be used by policymakers and the health care field, to assess the different levels and types of risk related to health IT and apply appropriate oversight mechanisms, in alignment with the principles and recommendations of the recently released BPC Report, An Oversight Framework for Assuring Patient Safety in Health Information Technology.

In order to achieve these outcomes, following the release of the BPC Report in February, BPC initiated a collaborative effort to further define health IT and develop a draft list of health IT functions. These functions reflect the concept of intended use, which the FDA uses to assess the applicability of appropriate regulatory requirements for medical devices. Collaborators also agreed that IT applications are diverse and that an attempt to assess risk must be based on function.

For each health IT function, collaborators provided a subjective assessment of the degree of patient safety risk and the category of oversight (based on the BPC oversight framework) that would most likely apply given the risk assessment.

There was also discussion as to how one would categorize an application with multiple functions (which could span multiple risk levels) to assess the overall risk category and associated oversight framework for the application. This issue continues to be actively discussed given current practice in the FDA-regulated space is to categorize an application based on the highest risk function. Such an approach might not be appropriate for products that are primarily comprised of clinical or administrative health IT functions. This matter requires further discussion and analysis.

The following is a summary of health IT definitions developed.

- **Medical Device Software**

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

  Examples include:

- Laboratory Information Systems
- Infusion Pumps
- Tumor measurement software

- **Clinical Software**

  Clinical software captures, analyzes or presents patient or population clinical data/information and may inform or recommend courses of patient specific clinical care. This class of HIT represents a low to moderate risk of patient harm.

  Examples include:

  - EHRs
  - Computerized physician order entry

- **Administrative Software**

  Administrative software supports the administrative and operational aspects of health care but is not used in direct delivery of clinical care. This includes population analytics that are not used for patient specific treatment or diagnosis. This class of HIT represents the lowest level of risk of patient harm.

  Examples include:

  - Scheduling software
  - Billing systems

The draft list of health IT functions and draft categorization of such functions within the BPC oversight framework are summarized in Appendix A and Appendix B. It should be noted that these documents are a work-in-progress, have not been agreed upon by all members of the collaborative effort, and are provided for illustrative purposes only.

Efforts are now underway to finalize the list of categorized health IT functions and extrapolate the subjective risk assessment effort into a generalized risk scoring model based on evaluation criteria that can be used to test and validate the subjective risk assessments.

Appendix A provides a list of functional use cases. Each functional use case has been assigned to one or more of the risk and oversight categories: Medical Device (MD), Clinical Software (CS) or Administrative Software (AS). The functional use cases were also assigned to one of 19 broad health IT functional categories outlined in Appendix B.

Appendix B shows that some functional categories span all three risk categories, while others-- such as “alerts” and “financials”--are assigned to a single risk category. This demonstrates that consideration of a more granular functional use case is necessary in developing a more generalized risk model.

BPC expects to finalize and make publicly available these work products when complete.

# Appendix A: Taxonomy of Health IT Functions (DRAFT)

| | | Potential Risk Category | | |
|---|---|---|---|---|
| **Intended Use** | **Category** | **MD** | **CS** | **AS** |
| Creates medication alergy alert | A | | x | |
| Creates medication interaction alert | A | | x | |
| Enter / view medication alergies for patient | A | | x | |
| Makes and records final order decision | A | | x | |
| Calculate and generate MU quality measures | AD | | | x |
| Conducts quality control checking of equipment | AD | x | | |
| Configures individual patient data trending requirements | AD | | x | x |
| Displays diagnostic test results | AD | | x | |
| Generates population analytics for non-patient specific use | AD | | | x |
| Generates population analytics for patient specific use | AD | | x | |
| Provides individual patient data trending | AD | | x | x |
| Submit patient data to third parties for clinical research purposes | AD | | | x |
| Communicate internal care transition plan | C | | x | |
| Completes patient survey | C | | | x |
| Provides secure messaging between/among clinicians and patients | C | | | x |
| Views/downloads billing data | C | | | x |
| Views/downloads clinical data | C | | x | |
| Communicates external care transition plan | CI | | x | |
| Generates clinical summary | CI | | x | |
| Generates external care transition plan (eligibility) | CI | | | x |
| Import medical device data (primary) | CI | x | | |
| Import medical device data (secondary) | CI | | x | |
| Imports diagnostic results | CI | | x | |
| Manage Internal networks | CI | | x | x |
| Receives internal clinical information exchange | CI | | x | |
| Transmits clinical information to third party | CI | | x | |
| Transmits internal clinical information exchange | CI | | x | |
| Acquires and displays patient data from longitudinal record | CM | | x | |
| Analyzes clinical data | CM | | x | |
| Create/Update/Utilize Care plans | CM | | x | |
| Creates plan for patient discharge | CM | | x | x |
| Displays patient tracking "boards" | CM | | x | x |
| Documents clinical task management | CM | | x | x |
| Generates care transition plan | CM | | x | x |
| Provides case management lookup information | CM | | x | |
| Provides lifestyle counseling | CM | | | x |

| | | | | |
|---|---|---|---|---|
| Provides patient wellness and lifestyle self management information | CM | | x | x |
| Reconciles clinical data | CM | | x | |
| Searches for patient data | CM | | x | |
| Self diagnosis | CM | x | x | x |
| Use patient treatment preference in clinical decision making | CM | | x | |
| Uses information for clinical management | CM | | x | |
| Uses patient wellness and lifestyle self management | CM | | x | x |
| Utilizes case management information | CM | | x | x |
| Views clinical data | CM | | x | |
| Views list of patients clinician is covering | CM | | | x |
| Enters patient order (diagnostic & treatment) | CPOE | | x | |
| Configures order sets | CR | | x | |
| Configures treatment protocols | CR | | x | |
| Displays and transmits order sets | CR | | x | |
| Displays and transmits treatment protocols | CR | | x | |
| Generates clinical reminders | CR | | x | |
| Performs clinical calculations | CR | | x | |
| Uses clinical data to generate clinical recommendation | CR | | x | |
| Creates permanent legal record | DC | | x | x |
| Dictates notes | DC | | x | x |
| Displays / records real time patient physiological data | DC | x | | |
| Documents clinical consultation | DC | | x | |
| Documents clinical summary of care | DC | | x | |
| Documents patient clinical information | DC | | x | |
| Documents patient consent and treatment preferences | DC | | | x |
| Documents patient response to treatment | DC | | x | |
| Records clinical data | DC | | x | |
| Records clinical information | DC | | x | |
| Records demographic data | DC | | | x |
| Records Unique Device Identifier | DC | | | x |
| Conducts utilization analysis | F | | | x |
| Conducts utilization reviews | F | | | x |
| Displays coding guidance | F | | | x |
| Displays reimbursement data from payor | F | | | x |
| Documents treatment justification for billing purposes | F | | | x |
| Generates business analyticals | F | | | x |
| Generates patient bill | F | | | x |
| Generates patient billing reminders | F | | | x |
| Provides contract management data for billing | F | | | x |
| Records payment / reconcilation | F | | | x |
| Transmits bill to payor | F | | | x |

| | | | | |
|---|---|---|---|---|
| Captures bed management data | FM | | | x |
| Documents equipment maintenance | FM | | | x |
| Maintains inventory | FM | | | x |
| Tracks equipment inventory | FM | | | x |
| Acquires/stores/displays diagnostic image data | IM | x | | |
| Acquires/stores/displays image storage and display for reference | IM | | x | |
| Manages clinical content for clinician reference | KM | | x | x |
| Creates legal medical record | L | | | x |
| Automatically controls medical device function | MDC | x | | |
| Automatically executes clinician orders | MDC | x | | |
| Controls medical device | MDC | x | | |
| Controls medical device | MDC | x | | |
| Controls surgical planning and control (robotics) | MDC | x | | |
| Captures data from diagnostic instruments (primary vs secondary) | MDD | x | | |
| Displays central patient monitoring | MDD | x | | |
| Generates alarms (physiological, technical or advisory) | MDD | x | | |
| Presents primary medical device data (directly from device) | MDD | x | | |
| Presents secondary medical device data (from primary system) | MDD | | x | |
| Provides remote monitoring of patient physiological data | MDD | x | | |
| Recommends radiation treatment plan | MDD | x | | |
| Records automated physical measurement | MDD | x | | |
| Accepts order / documents and dispenses drug | MM | | x | |
| Adminsters / records drug administration | MM | | x | |
| Dispenses drugs to clinician | MM | | x | |
| Manages drug distribution (logistics) | MM | | | x |
| Orders medication | MM | | x | |
| Supports telemedicine | O | x | x | x |
| Manages patient administrative master data | PID | | | x |
| Provides patient matching algorithms | PID | | x | |
| Documents patient safety event and treatment | RM | | | x |
| Manages patient safety event management | RM | | | x |
| Tracks, trends and reports on patient safety events | RM | | | x |
| Creates patient appointment | S | | | x |
| Generates appointment Reminders | S | | | x |
| Processes patient admission | S | | | x |
| Request appointment | S | | | x |
| Schedules and documents post discharge placement | S | | x | x |
| Schedules equipment for patient care | S | | | x |
| Schedules facility for patient care | S | | | x |
| Schedules staffing | S | | | x |

# Appendix B: List of Functional Categories and Corresponding Levels of Oversight (DRAFT)

| Category | Description | Proposed Oversight Model | | |
|---|---|---|---|---|
| | | Medical Device | Clinical Software | Administrative Software |
| A | Alerts | | | |
| AD | Analyze Data/Reporting | | | |
| C | Communication | | | |
| CI | Clinical Interoperability | | | |
| CM | Clinical Management | | | |
| CPOE | Order Entry | | | |
| CR | Clinical Recommendations | | | |
| DC | Data Capture | | | |
| F | Financials | | | |
| FM | Facility Management | | | |
| IM | Image Management | | | |
| KM | Knowledge Management | | | |
| L | Legal Record | | | |
| MDC | Medical Device Control | | | |
| MDD | Medical Device Data | | | |
| MM | Medication Management | | | |
| PID | Patient Identification | | | |
| RM | Risk Management | | | |
| S | Scheduling | | | |

# About the Bipartisan Policy Center's Health Innovation Initiative

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole, and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation, and respectful dialogue.

In collaboration with BPC's Health Project, which is led by former Senate Majority Leaders Tom Daschle (D-SD) and Bill Frist (R-TN), the Health Innovation Initiative conducts research and collaborates with experts and stakeholders across every sector of health care to develop recommendations that promote innovation and the use of IT to support improvements in the cost, quality, and patient experience of care.

Key areas of focus include the following:

1. Advancing the information foundation for delivery system and payment reforms and other population improvement efforts to promote higher quality, more cost-effective, patient-centered care.
2. Accelerating electronic health information sharing across the multiple settings in which care and services are delivered to support coordinated, accountable, patient-centered care that results in better outcomes in quality and cost.
3. Engaging consumers in their health and health care using electronic tools to improve quality, reduce costs, and improve the experience of care.
4. Assuring patient safety in the development and use of health IT, while preserving an environment that fosters the innovation needed for health IT to meet the needs of a rapidly changing health care system.
5. Accelerating innovation and providing an information foundation for personalized and genomic medicine.
6. Identifying and advancing innovative strategies for use by employers to improve health and wellness, and improve the quality and cost-effectiveness of care.

# Acknowledgements

BPC would also like to thank the following organizations, which contributed the time and expertise of their staff to the development of the principles and recommendations included in the BPC Report, An Oversight Framework for Assuring Patient Safety in Health Information Technology, from which a majority of the comments contained in this paper were drawn.

Aetna

Alliance for Quality Improvement and Patient Safety

Allscripts

American Academy of Family Physicians

American Academy of Pediatrics

American Cancer Society

American College of Cardiology

American College of Emergency Physicians

American College of Physician Executives

American College of Physicians

American College of Surgeons

American Congress of Obstetricians and Gynecologists

American Medical Group Association

American Medical Informatics Association

American Nurses Association

American Osteopathic Association

American Society of Clinical Oncology

Ascension Health

Association of American Medical Colleges

Association of Clinicians for the Underserved

Association of Medical Directors of Information Systems

athenahealth

AT&T

Baylor Health System

Blue Cross Blue Shield Association

Brookings Institution

CentraStateHealth System

Cerner Corporation

CHIME

Continua Health Alliance

Dell

Dignity Health

ECRI Institute

e-MDs

GE Healthcare

Geisinger Health System

Greenway Medical Technologies

HCA Healthcare

Health Fidelity

Healthcare Leadership Council

Health Level Seven

HIMSS

IBM Corporation

Intel Corporation

Intermountain Healthcare

Joint Commission

Kaiser Permanente

McKesson Corporation

Medical Group Management Association

Medtronic

National Association of Childrens' Hospitals and Related Institutions

National Association of Public Hospitals and Health Systems

National Coalition for Cancer Survivorship

National Medical Association

National Partnership for Women and Families

National Patient Safety Foundation

National Rural Health Association

NewYork Presbyterian Hospitals

NextGen HealthCare

North Shore-LIJ Health System and Hofstra North Shore-LIJ School of Medicine

Philips Healthcare

Poudre Valley Medical Group and Poudre Valley Health System

Practice Fusion

Premier

Qualcomm

Sharp HealthCare

Siemens Healthcare

Summit Health Institute for Research and Education (SHIRE)

Tenet Healthcare Corporation

Tennessee Office of eHealth Initiatives

Texas Office of eHealth Coordination

United Health Group

University of Texas at Houston

Vanderbilt University School of Nursing

# Endnotes

[1] Institute of Medicine. (1999). *To Err is Human*. Washington, D.C.: The National Academies Press.

[2] Institute of Medicine. (2001). *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, D.C.: The National Academies Press.

[3] Buntin M.B., Burke M., Hoaglin M., and Blumenthal D. (2011). The Benefits of Health Information Technology: A Review of the Recent Literature Shows Predominantly Positive Results. *Health Affairs*, 30(3): 464–471.

[4] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.

[5] Pennsylvania Patient Safety Authority. (2012). *The Role of Electronic Health Records in Patient Safety Events*.

[6] Buntin M.B., Burke M., Hoaglin M., and Blumenthal D. (2011). The Benefits of Health Information Technology: A Review of the Recent Literature Shows Predominantly Positive Results. *Health Affairs*, 30(3): 464–471.

[7] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.

[8] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.

[9] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.

[10] Institute of Medicine. (1999). *To Err is Human*. Washington, D.C.: The National Academies Press.

[11] OMB Circular No. A-119.

[12] OMB Circular No. A-119.

[13] National Technology Transfer and Advancement Act of 1995.

[14] ECRI Institute. (2012). ECRI Institute PSO Deep Dive: Health Information Technology. Plymouth Meeting, PA: ECRI Institute.

[15] National Association of State Health Policy. (2012).

[16] Joint Commission on Accreditation of Healthcare Organizations (2012). Comprehensive Accreditation Manual for Hospitals, Update 1, March 2012. JCAHO: Chicago, IL.

[17] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.

[18] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press.