Health Program
Health Project

An Oversight Framework for Assuring Patient Safety in Health Information Technology

Bipartisan Policy Center Health Innovation Initiative

February 2013

BIPARTISAN POLICY CENTER

Health Program

Health Project

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

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 information technology (IT) plays in improving the quality and safety of care. Because greater use of health IT has always had strong bipartisan support, members of Congress and leaders across two administrations have taken significant actions to increase the adoption of IT to improve the quality, safety, and cost-effectiveness of health care.

Building upon numerous legislative proposals with bipartisan support over the last decade, the Health Information Technology and Economic and Clinical Health (HITECH) Act of 2009 brought about new authorities, standards, and investments in health IT. As a result of federal, state, and private-sector action, the number of clinicians, hospitals, and other providers across the United States who have adopted health IT to improve the quality, safety, and efficiency of care has significantly increased.

The widespread adoption of health IT largely stems from recognition of the important role that it plays in improving health care quality and safety. However, there are also instances in which it has the potential to create harm if not effectively developed, implemented, or used. Nonetheless, a recent IOM report indicated that health information systems were involved in less than 1 percent of reported errors in health care settings.[3]

Policies are now being developed by the Department of Health and Human Services (HHS) to use health IT to make health care safer and continuously improve the safety of health IT. HHS released for public comment on December 21, 2012, the *Health IT Patient Safety Action and Surveillance Plan for Public Comment*, which represents the administration's proposed approach for addressing safety in health IT. The Food and Drug Administration (FDA) Safety and Innovation Act of 2012, which was passed by Congress and signed into law in July 2012, calls for the HHS secretary to develop—within 18 months—a proposed strategy and recommendations on risk-based regulatory framework pertaining to health IT that promotes innovation, protects patient safety, and avoids regulatory duplication.[4]

Through a collaborative effort, the Bipartisan Policy Center (BPC) has both conducted research and engaged a wide range of experts and stakeholders to develop a set of principles and recommendations for an oversight framework for assuring patient safety in health IT. The framework 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.

Principles for an Oversight Framework for Assuring Patient Safety in Health IT

The following set of principles, which were developed through a collaborative process involving experts and stakeholders across every sector of health care, 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 Assuring Patient Safety in Health IT

Assuring patient safety in the development, implementation, and use of health IT requires both national focus and public- and private-sector collaboration and leadership.

Health IT broadly falls into three major categories, each of which reflects increasing levels of risk of potential patient harm: (1) administrative or non-clinical software, (2) clinical software, and (3) medical device software. The primary factors that should be used to determine the level of oversight for any type of software include the level of risk of potential patient harm and, for clinical software, the degree of direct clinical action on patients.

Assuring safety in clinical software in particular is a shared responsibility among developers, implementers, and users across the various stages of the health IT life cycle, which include design and development; implementation and customization; upgrades, maintenance, and operations; and risk identification, mitigation and remediation.

Clinical software includes electronic health records, clinical decision support software, and other software used to inform clinical decision-making. Such software should be subject to a new oversight framework, rather than traditional regulatory approaches applied to medical

devices given its lower risk profile taking into account several factors. These factors include the level of risk of potential patient harm, the degree of direct clinical action on patients, the opportunity for clinician involvement, the nature and pace of its development, and the number of factors beyond the development stage that impact its level of safety in implementation and use. This oversight framework should contain four main elements summarized below.

1. Agreement on and adherence to 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, including reporting, analysis, and response, while leveraging patient safety organizations (PSOs).
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.

HHS's current proposed approach—outlined in *Health IT Patient Safety Action and Surveillance Plan for Public Comment*, which was released on December 21, 2012—reflects many of the key elements outlined above, including development of and adherence to standards and guidelines; reporting and analysis of, and response to patient safety events in a non-punitive environment to support mitigation of risk, as well as learning and improvement; and research and implementation support for users, developers, and implementers.

As HHS develops its proposed strategy and recommendations for a risk-based, regulatory framework for health IT, BPC urges the department to consider the principles and recommendations for an oversight framework for health IT outlined above and within this report.

Introduction

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.[5,6] Both reports highlighted the critical role that health information technology (IT) plays in improving the quality and safety of care. Because greater use of health IT has always had strong bipartisan support, members of Congress and leaders across two administrations have taken significant actions to increase the adoption of IT to improve the quality, safety, and cost-effectiveness of health care.

Today, health care costs constitute 18 percent of our nation's gross domestic product and the quality of care remains uneven. 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. 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.[7]

Building upon numerous legislative proposals with bipartisan support, the Health Information Technology and Economic and Clinical Health (HITECH) Act of 2009 brought about new authorities, standards, and investments in health IT. Numerous states and private-sector health plans have also implemented policies that promote the adoption and use of health IT. As a result of these efforts, the percentage of office-based physicians who have adopted a basic electronic health record (EHR) has more than tripled in the last five years, totaling 40 percent in 2012.[8] In 2011, 18 percent of hospitals had a basic EHR system in place, up from 11.5 percent the previous year.[9] Many clinicians, hospitals, and other providers have qualified for funding under the Centers for Medicare and Medicaid Services (CMS) EHR Incentive Programs by demonstrating the meaningful use of EHR technology to improve care. As of December 31, 2012, more than $10.7 billion in payments had been made through these incentive programs to approximately 3,500 hospitals and more than 186,000 eligible professionals.[10]

The widespread adoption of health IT largely stems from recognition of the important role that it plays in improving health care quality and safety. However, there are also instances in which it has the potential to create harm if not effectively developed, implemented, or used. A recent IOM report indicated that health information systems were involved in less than 1 percent of reported errors in health care settings.[11] 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.[12]

Policies are now being developed by the Department of Health and Human Services (HHS) to use health IT to make health care safer and to continuously improve the safety of health

IT. The Office of the National Coordinator for Health IT (ONC) commissioned an IOM study on how government and the private sector can maximize the safety of health IT-assisted care. The report, *Health IT and Patient Safety: Building Safer Systems for Better Care*, was released in November 2011. On December 21, 2012, HHS released *Health IT Patient Safety Action and Surveillance Plan for Public Comment*, which represents the administration's proposed approach for addressing safety in health IT.

The Food and Drug Administration (FDA) Safety and Innovation Act of 2012, which was passed by Congress and signed into law in July 2012, requires the HHS secretary, "acting through the Commissioner of Food and Drugs, and in consultation with the National Coordinator for Health Information Technology and the Chairman of the Federal Communications Commission," to post a report within 18 months that "contains a proposed strategy and 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."[13]

Through a collaborative effort, the Bipartisan Policy Center (BPC) has both conducted research and engaged a wide range of experts and stakeholders—including clinicians, consumers, employers, health plans, hospitals, quality and patient safety organizations, academic and research institutions, and technology companies—to inform federal policy related to patient safety and health IT. As a result of the review of the literature and more than 40 meetings involving nearly 100 organizations representing diverse interests in health care, BPC has developed a set of principles and recommendations for an oversight framework for assuring patient safety in health IT. The framework 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.

Chapter 1: Principles for a Framework for Assuring Safety in Health IT

The following set of principles, developed through a collaborative process involving experts and stakeholders across every sector of health care, should guide the federal government's development of an oversight framework for assuring patient safety in 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.[14] 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.[15] This larger system includes technology, people, processes, organizations, and the external environment.[16]

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."[17] Lessons learned from such other approaches should be integrated into any oversight framework for health IT.

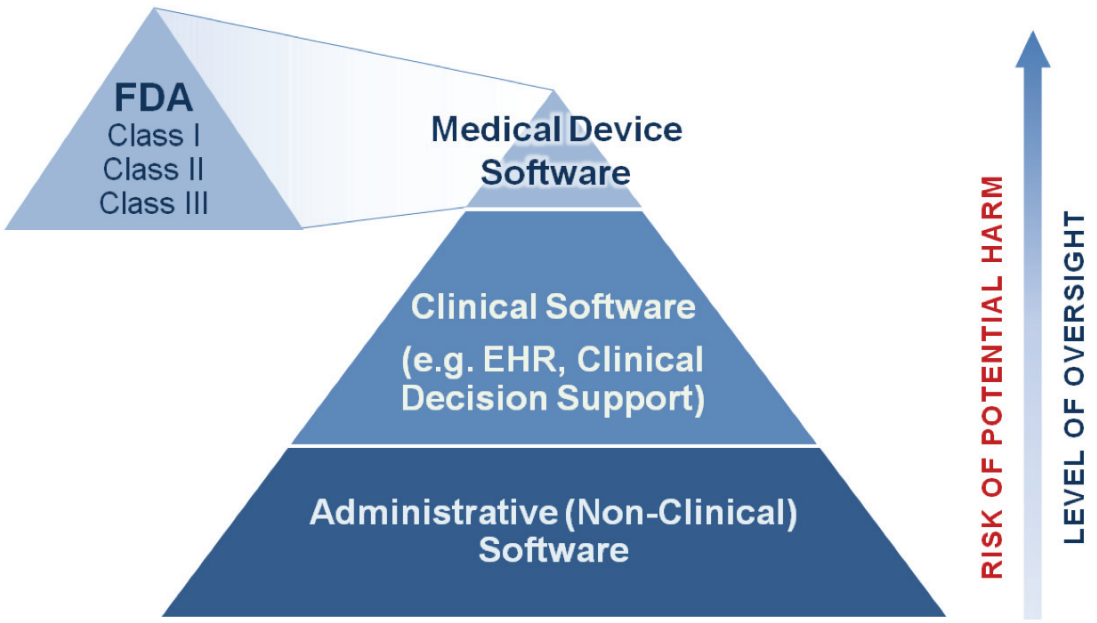
Chapter 2: Key Elements of an Oversight Framework for Assuring Safety in Health IT

Assuring patient safety in health IT is best accomplished through an oversight framework that reflects the principles outlined in this report. The framework should be risk-based and reflect shared responsibility, promote innovation, be flexible to accommodate a rapidly changing health care system, support learning and improvement, and leverage existing safety and quality-related processes, systems, and standards.

A Framework for Oversight Based on Risk

Health IT broadly falls into three primary categories (illustrated in Figure 1 below), each of which reflects increasing levels of risk of potential patient harm: (1) administrative or non-clinical software, (2) clinical software, and (3) medical device software.

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



Administrative software—which supports the administrative and operational aspects of health care but is not used in the direct delivery of care—represents the category with the lowest level of risk of potential patient harm. One example of administrative software is scheduling software, which enables health care providers to schedule appointments with patients. Based on the level of risk of patient harm associated with such software, additional oversight is not warranted.

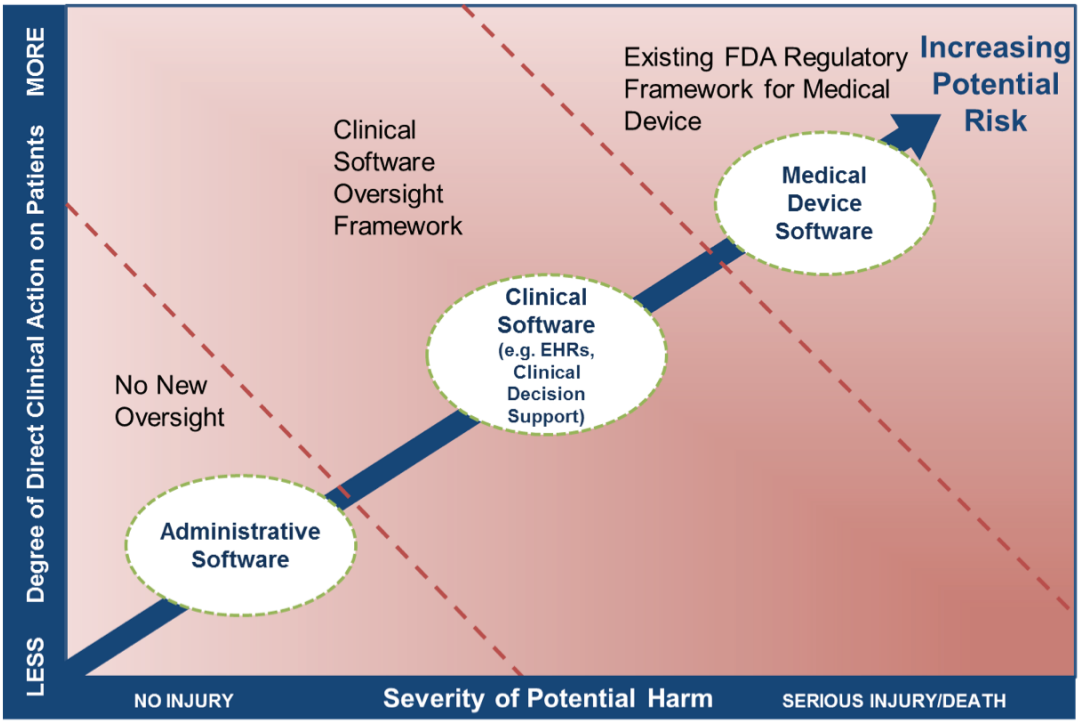
Clinical software informs clinical decision-making and directly supports the delivery of care to patients. Examples include EHRs, computerized physician order entry, and clinical decision support software.

Finally, medical devices, including medical device software, represent a high potential risk of patient harm and in most cases, directly interact with the patient with little or no opportunity for clinical intervention. Examples of traditional medical devices include pacemakers, electrocardiograms, automated external defibrillators, and mammography computer-aided detection systems. Such devices are currently regulated by the FDA as Class I, Class II, or Class III medical devices.

Determining the Level of Oversight

As illustrated in Figure 2, factors used to determine the type of oversight to be applied include: the level of risk of potential patient harm and the degree of direct clinical action on patients.

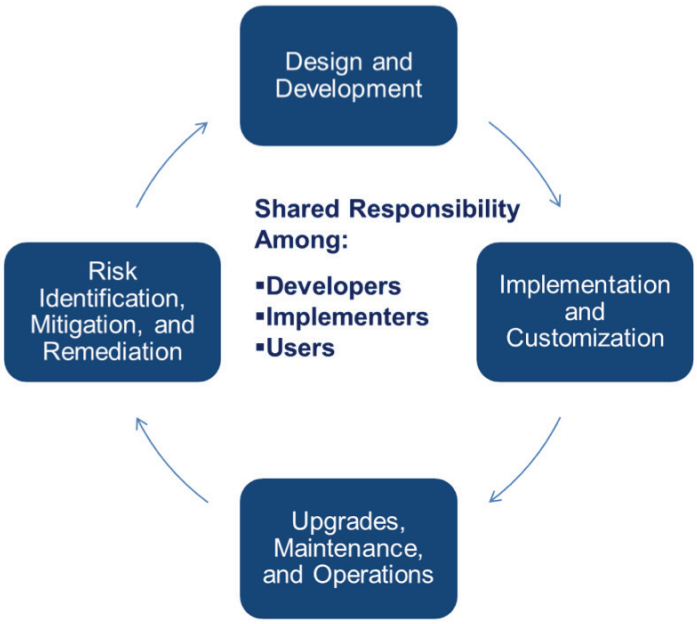
Figure 2. Factors That Determine Level of Oversight



The FDA's current regulatory approach for medical devices is generally not well-suited for health IT. Unlike medical devices, health IT relies not only on how it is designed and developed, but also on how it is customized, implemented, and used. Safety of medical devices is almost entirely dependent on how they are manufactured by developers—which is the focus of medical device regulation. Safety in health IT, however, is a shared responsibility among developers, implementers, and users across the various stages of the health IT life cycle, which include design and development; implementation and customization; upgrades, maintenance, and operations; and risk identification, 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



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. Unlike medical devices, health IT is designed to inform—not take the place of—clinical decision-making. Clinical software does not directly interact with patients as medical devices often do. Health IT supports but does not replace

the judgment of clinicians. When using health IT for clinical care, clinicians ultimately retain clinical judgment and discretion.

Another differentiation between medical devices and health IT is that 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. Federal and state agencies as well as private-sector payers are increasingly calling upon clinicians, hospitals, and other providers to bolster health IT capabilities to support the implementation of new delivery system and payment reforms, as well as requirements for health IT incentive programs—such as those associated with CMS' Medicare and Medicaid EHR Incentive Programs. Constantly evolving systems, such as health IT, don't lend themselves to discontinuous oversight mechanisms such as those used for medical devices.

Key Elements of the Oversight Framework for Clinical Software

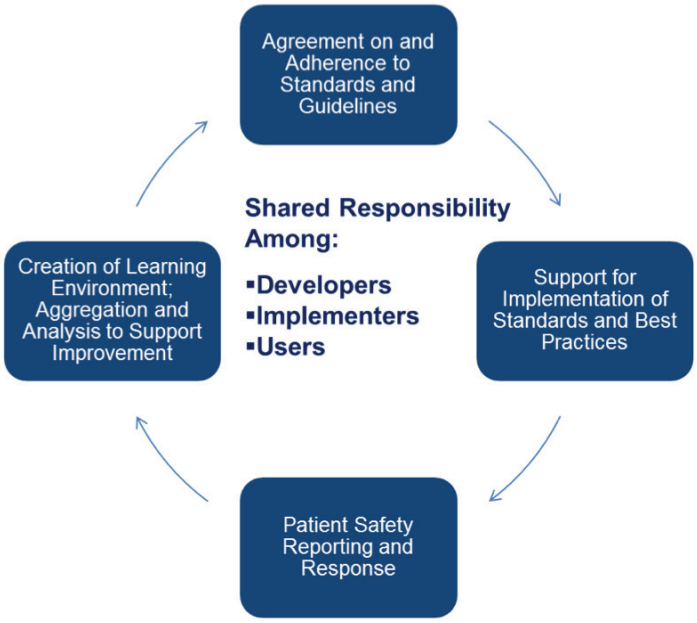
Assuring patient safety in the use of health IT—and in particular, clinical software—requires both national focus and public- and private-sector collaboration and leadership. As noted previously, this is best accomplished through an oversight framework that is not only risk-based and reflects shared responsibility, but also one that promotes innovation, is flexible to accommodate a rapidly changing health care system, supports learning and improvement, and leverages existing safety and quality-related processes, systems, and standards.

As illustrated in Figure 4 below, the oversight framework for the safe use of clinical software should be composed of four main elements:

1. Agreement on and adherence to 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 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.

Addressing these four elements is a shared responsibility among developers, implementers, and users of clinical software.

Figure 4. Oversight Framework for Patient Safety in Clinical Software



Alignment with HHS-Proposed Health IT Patient Safety Action and Surveillance Plan

The oversight framework for assuring patient safety in health IT outlined in this report aligns with the approach proposed in HHS' *Health IT Patient Safety Action and Surveillance Plan for Public Comment* in several ways, including: the focus on leveraging existing programs and processes, development of and adherence to standards, reporting and response by providers and health IT developers, aggregation and analysis of patient safety events to facilitate improvement, and provision of implementation support through research and development of user tools and best practices related to safety and health IT. As described in more detail below, the oversight framework relies on a process-oriented approach. The HHS plan calls for the use of process standards, but does so within the context of a product-focused EHR certification program.

A more detailed description of each element of the oversight framework for clinical software is provided below, along with recommendations that will speed its implementation.

Chapter 3: Recommendations for an Oversight Framework for Safety in Health IT

1. Agreement on and Communication of a Health IT Safety Oversight Framework That Reflects Shared Principles and Builds upon Key Elements Addressed in This Report

HHS has taken important steps to advance patient safety in health IT–enabled care. First, it commissioned an IOM study on how government and the private sector can maximize the safety of health IT–assisted care. Second, on December 21, 2012, it published *Health IT Patient Safety Action and Surveillance Plan for Public Comment,* which represents the administration's proposed approach to patient safety in health IT. The administration's proposed action plan aligns with many of the principles outlined in this report and signals its intention to manage the oversight of health IT outside of the traditional medical device regulatory regime.

The FDA Safety and Innovation Act of 2012, which was passed by Congress and signed into law in July 2012, calls for the HHS secretary to post—within 18 months—"a report that contains a proposed strategy and 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."[18]

The possibility of government regulation in health IT has the potential of stifling innovation and much-needed investment in an industry that must significantly expand, evolve, and innovate to support the growing demands of a health care system that is undergoing considerable modernization and transformation to address continuing concerns about rising health care costs and uneven quality.

Imposing a new set of regulations in the midst of a health care environment that is already fiscally challenged and facing many new regulations and requirements brought about by the Affordable Care Act and HITECH, has the potential to overwhelm the system.

At the same time, clinicians, hospitals and other providers, technology companies, and patients are seeking agreement and collaborative action on a set of principles, guidelines, processes, and systems that will support them in both using health IT to improve patient safety and improving the safety of health IT–assisted care.

BPC has both conducted research and engaged a wide range of experts and stakeholders to inform this set of recommendations for an oversight framework for assuring patient safety in health IT.

Recommendation 1.1

As HHS finalizes its patient safety action and surveillance plan and develops its proposed strategy and recommendations for a risk-based, regulatory framework for health IT, we urge the department to consider the principles and recommendations for an oversight framework included in this report.

The oversight framework for patient safety should reflect the following key principles:

1. 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. Recognize that assuring patient safety, along with positive patient outcomes, is a shared responsibility that must involve the entire health care system.
3. Be risk-based, flexible, and do not stifle innovation.
4. Leverage existing safety and quality-related processes, systems, and standards.
5. Recognize that reporting of patient safety events is essential and that a non-punitive environment should be established to encourage reporting, learning, and improvement.

The oversight framework should enable national focus and public- and private-sector collaboration and leadership. Rather than rely upon existing approaches for the regulation of medical devices, the oversight framework for clinical software should call upon developers, implementers, users, PSOs, and experts, working in collaboration with government, to:

1. Agree upon and promote adherence to—through accreditation, as appropriate--recognized standards and guidelines for assuring patient safety in the development, implementation, and use of health IT.

2. Provide support for the implementation of such standards and guidelines as well as develop and disseminate best practices, through education, training, and technical assistance.
3. Enable developer, implementer, and user participation in patient safety activities, leveraging PSOs, including reporting, analysis, and response.
4. Create a learning environment; aggregate and analyze non-identified patient safety reports to identify and monitor trends, mitigate future risk, and facilitate learning and improvement.

A description of each component of the oversight framework for clinical software and recommendations for the actions needed to support implementation are summarized below.

2. Agreement on and Adherence to Recognized Standards and Guidelines for Assuring Patient Safety

One of the key components of the oversight framework is a process for gaining agreement on process standards and guidelines for assuring patient safety in the development, implementation, and ongoing use of health IT. 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.

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 functionality, such as those that play a predominant role within current EHR certification programs associated with CMS' Medicare and Medicaid EHR Incentive Programs. 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.[19]

Well-established international standards that enable patient safety already exist and are developed under the auspices of the International Organization for Standardization (ISO). Examples of such existing process standards include those that address quality-management systems (ISO 9001), product risk management (ISO 14971), software development (ISO 62304), and usability (ISO 62366). The development of a new ISO standard focused on assuring the safer development, implementation, and operation of health software is currently underway.[20] 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.

Finally, 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.

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.[21] 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.[22,23]

Recommendation 2.1

Independent, voluntary consensus bodies should engage developers, implementers, users, health IT and safety experts, and consumers to gain ongoing agreement on a set of standards and guidelines for assuring patient safety in the design, development, implementation, and use of health IT.

Recommendation 2.2

Independent voluntary consensus bodies and organizations that represent developers, implementers, users, and patient safety and health IT experts should collaborate on the dissemination of agreed-upon standards and guidelines as well as on the development and delivery of educational programs and implementation support services designed to educate and promote compliance with such standards and guidelines.

Recommendation 2.3

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.

Recommendation 2.4

Existing, independent provider accreditation bodies should be evaluated for their reference and support of recognized standards and guidelines for software implementation and use.

3. Support for Implementation of Standards and Guidelines; Development and Dissemination of Best Practices for Developers, Implementers, and Users

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.

Developers, implementers, and users will increasingly need to work together to develop strategies that meet the growing demands of a rapidly changing health care system. 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.

Recommendation 3.1

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 in 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.

4. Participation in Patient Safety Activities Including Reporting, Analysis, and Response

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.

LEVERAGING EXISTING PATIENT SAFETY-RELATED AUTHORITIES, ORGANIZATIONS, AND PROCESSES

Congress passed the Quality Safety and 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.

The Patient Safety Act authorized the creation of patient safety organizations (PSOs). PSOs, which must be certified for listing and evaluated on an ongoing basis by the Agency for Healthcare Research and Quality (AHRQ), serve as patient safety experts and receive data regarding patient safety events that are considered privileged and confidential.[24]

Currently, 88 PSOs are listed on the AHRQ website, representing a range of for-profit and not-for-profit organizations and entities that are components of other organizations, such as hospital associations, medical societies, or health systems.[25]

Rather than establish new authorities or structures for reporting and analysis of patient safety events specific to health IT, PSOs—who are already authorized to serve as patient safety experts and receive data regarding patient safety events that are considered privileged and confidential—should be leveraged to support reporting for patient safety events associated with health IT.

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.[26]

Recommendation 4.1

Authorities, structures, and organizations brought about by the Patient Safety and Quality Improvement Act—including patient safety organizations—should be leveraged to support reporting and analysis of health IT–related patient safety events.

ENABLING DEVELOPERS TO PARTICIPATE IN PATIENT SAFETY ACTIVITIES

The Patient Safety Act establishes a culture of safety for providers by providing statutory confidentiality protections for "patient safety work product" (PSWP). Specifically, identifiable patient safety work product is defined, in part, as PSWP that is presented in a form and manner that allows the identification of any provider that is a subject of the work product, or any providers that participate in activities that are a subject of the work product (42 USC 299b-21(2)) .

This provision grew out of the 1999 IOM Report *To Err is Human*, which reported that without protections providers did not share information about errors and thus the errors were repeated. The culture of safety permits providers to participate in activities intended to improve the quality of patient care without fear of liability or harm to professional reputation. Importantly, this provision does not exempt the provider from lawsuits; information in the medical record concerning the underlying facts is not protected under the Patient Safety Act and remains available to plaintiffs, just as it was before the passage of the Act.

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 safety is a shared responsibility, developers should participate in the reporting of patient safety events, just as providers do. 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.[27] 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.[28] Like providers, developers can be reluctant to report out of fear of legal liability or harm to reputation.

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.

Recommendation 4.2

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.

Recommendation 4.3

The Agency for Healthcare Research and Quality 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

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.

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

Patient safety event reporting, analysis, identification of root cause, and corrective action are critical to improving patient safety in health IT-assisted care. Those who develop, implement, and use health IT should be encouraged to report patient safety events to facilitate learning and improvement and mitigate future risk.

Recommendation 4.4

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.

Recommendation 4.5

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.

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 traditional PSO activities—such as 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.

As clinicians, hospitals and other providers, and developers increasingly begin to rely on PSOs for the reporting of patient safety events that are or may be associated with health IT, they will expect that PSOs offering such services will have the expertise and capabilities

associated with this new and emerging field. While baseline knowledge and capabilities should be expected of all PSOs, demonstration and communication of advanced capabilities will help developers, implementers, and users identify PSOs with which they wish to establish a relationship to support reporting of patient safety events associated with health IT. Demonstration of such advanced capability could be accomplished through a PSO-led accreditation program associated with health IT–related patient safety events, with support by developers, implementers, users, and experts in both patient safety and health IT.

Recommendation 4.6

PSOs, developers, implementers, users, and health IT and patient safety experts should collaborate on the development of standards, guidelines, strategies, and best practices for collecting, analyzing, and investigating health IT–related patient safety events; defining corrective action and providing timely feedback; and taking other actions as necessary to mitigate future risk and facilitate learning and improvement.

Recommendation 4.7

PSOs should collaborate with developers, implementers, users, and patient safety and health IT experts on the development and launch of an accreditation program that reflects established standards, guidelines, and best practices and promotes effective implementation of patient safety activities related to health IT. PSOs that wish to specialize in health IT–related patient safety activities should undergo such accreditation.

5. Creation of a Learning Environment for Safety in Health IT

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.

To support PSOs and providers in their efforts to develop and adopt improvements in patient safety, the Patient Safety Act authorized AHRQ to facilitate the development of a network of patient safety databases (NPSD), to which PSOs, health care providers, or others can voluntarily contribute non-identifiable patient safety work product. By facilitating the aggregation and analysis of data nationwide, the NPSD is intended to assist PSOs and providers in their efforts to develop and adopt improvements in patient safety.[29]

Another way in which aggregation, analysis, and improvement activities can take place with the support of confidentiality protections under the Patient Safety Act is through the aggregation and analysis of non-identified patient safety from numerous PSOs into another

PSO that focuses on aggregation and analysis. As patient safety reporting for health IT takes hold, it is likely that a combination of the two scenarios identified above will emerge.

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.

Recommendation 5.1

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.

ENCOURAGING USE OF STANDARD FORMATS FOR REPORTING AND RESPONSE

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.

As noted previously, the Patient Safety Act requires PSOs—to the extent practical and appropriate—to collect patient safety data from providers in a standardized manner. If providers or PSOs choose to submit patient safety data to the NPSD, AHRQ requires that these data be submitted using the AHRQ Common Formats, which are common definitions and reporting formats used to facilitate the collection and reporting of patient safety events. To date, AHRQ has developed Common Formats for two settings of care—acute care hospitals and skilled nursing facilities. Future versions of the Common Formats are being developed for ambulatory settings. AHRQ has also developed Common Formats to support the reporting of patient safety events related to health IT.[30]

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 either to a PSO or the NPSD should be encouraged to utilize standardized formats. To the extent feasible and appropriate, the AHRQ Common Formats should be leveraged to support reporting using standardized formats.

Recommendation 5.2

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

Recommendation 5.3

Given the increase in adoption of EHRs among clinicians in ambulatory settings and given the critical importance of patient safety reports from such environments—particularly as it relates to health IT, AHRQ should continue and accelerate its efforts to develop Common Formats for ambulatory care.

Recommendation 5.4

To facilitate the aggregation and analysis of patient safety data to support learning and improvement in the area of health IT, PSOs should explore aggregating patient safety events associated with health IT either through reporting to the NPSD or to another PSO that is aggregating such data to support learning and improvement.

Conclusion

Health IT plays a critical role in improving the quality, safety, and cost-effectiveness of care. Continuing to use health IT to make health care safer and assuring the safety of health IT is essential. Through the implementation of the principles and recommendations summarized in this report, the federal government, states, and private-sector leaders across every sector of health care can make significant strides in achieving these dual goals, while continuing to improve how health care is delivered in the United States.

As policy makers consider the development of a regulatory framework for health IT, we urge them to consider the oversight framework outlined in this report, which 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 thanks the many organizations and individuals, listed in the acknowledgements section of this report, who contributed their time and expertise to the development of principles and recommendations included in this report.

Through the BPC Health Innovation Initiative, we plan to continue the dialogue on the principles, policies, and strategies that should be adopted to promote the use of health IT to improve patient safety, while assuring safety in the development, implementation, and use of health IT.

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, BPC is a nonprofit 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. See www.bipartisanpolicy.org.

In coordination with BPC's Health Project, which is led by Health Project co-leaders and 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 health care to develop recommendations that promote innovation as well as the use of IT to drive improvements in the cost, quality, and patient experience of care. Key areas of focus include the following:

1. Creating the information foundation for delivery system and payment reforms that promote higher-quality, more cost-effective care.
2. Expanding engagement of consumers in their health and health care to improve outcomes in cost, quality, and patient experience of care.
3. Accelerating the electronic exchange of health information across the multiple settings in which care and services are delivered to support coordinated, accountable, patient-centered care that improves quality and reduces costs.
4. Assuring privacy and security of electronic health information by gaining agreement among stakeholders in health care on a set of principles, policies, and strategies for managing privacy as it relates to both the delivery of care and improvements in population health.
5. Assuring patient safety in health IT, while preserving an environment that fosters the innovation needed for a rapidly changing health care system.
6. Advancing innovation in new areas that will promote better outcomes in quality and cost, including those related to personalized and genomic medicine.

Acknowledgements

BPC would like to thank Janet Marchibroda, director of the BPC Health Innovation Initiative; Katie Golden, BPC health policy analyst; and Ann Gordon, writer and editor, for their contributions to this report.

BPC would also like to thank the following organizations, which contributed their time and expertise to the development of the principles and recommendations included in this report.

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

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 Children's 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] Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care.* Washington, D.C.: The National Academies Press, 187.

[4] Food and Drug Administration Safety and Innovation Act of 2012.

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

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

[7] 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.

[8] Hsiao C. and Hing E. (2012). Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices: United States, 2011–2011. *NCHS Data Brief*; *111*. Hyattsville, MD: National Center for Health Statistics.

[9] DesRoches C.M., Worzala C., Joshi M.S., Kravolec P.D., and Jha A.K. (2012). Small, Nonteaching, and Rural Hospitals Continue to be Slow in Adopting Electronic Health Record Systems. *Health Affairs*, 31(5).

[10] Centers for Medicare and Medicare Services. (2012). *Summary Report of CMS Medicare and Medicaid EHR Incentive Programs through December 2012*.

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

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

[13] Food and Drug Administration Safety and Innovation Act of 2012.

[14] 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.

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

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

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

[18] Food and Drug Administration Safety and Innovation Act of 2012.

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

[20] International Organization for Standardization. (2012). ISO TR 17791, Health Informatics Technical Report Guidance on Standards for Enabling Safety in Health Software. Geneva, Switzerland: International Organization for Standardization.

[21] OMB Circular No. A-119.

[22] OMB Circular No. A-119.

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

[24] The Patient Safety and Quality Improvement Act of 2005.

[25] Agency for Health Care Research and Quality. (2012). Agency for Healthcare Quality and Research Web Site: PSO FAQs. Accessed January 28, 2013.

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

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

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

[29] The Patient Safety and Quality Improvement Act of 2005.

[30] Agency for Health Care Research and Quality. (2012). Agency for Healthcare Quality and Research Web Site: PSO FAQs. Accessed January 28, 2013.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG