

HEALTH IT SAFETY CENTER ROADMAP

Collaborate on solutions, Informed by evidence



PREPARED FOR

**Office of the National Coordinator for Health
Information Technology**

US Department of Health and Human Services

Kathy Kenyon, Project Officer

PREPARED BY

RTI International

3040 E. Cornwallis Road

Research Triangle Park, NC 27709

CONTRACT NUMBER

HHSP23320095651WC_HHSP23337047T

Deliverable 2.4.4.

RTI PROJECT NUMBER

0212050.042.001.002

[This page intentionally left blank.]

ACKNOWLEDGMENTS

RTI International thanks the Health IT Safety Center Roadmap task force members for their time and input during the development of this roadmap. Their participation in task force meetings and work groups, and contributions across all sections of this roadmap, are greatly appreciated. In addition, we thank Gil Kuperman for his review and comments on this roadmap.

[This page intentionally left blank.]

CONTENTS

Section	Page
Executive Summary	1
1. Introduction	1
1.1 Background	1
1.2 The Need for a National Health IT Safety Center	2
2. Approach to Developing the Roadmap	5
3. Center Overview	7
3.1 Vision, Mission, and Objectives	7
3.2 Center Attributes	7
3.3 Center Stakeholders.....	8
4. Center Focus Areas, Activities, and Core functions	11
4.1 Focus Areas and Activities.....	11
4.2 Core Functions	13
5. Operations	15
5.1 Operations Overview	15
5.2 Center Roles and Responsibilities	16
5.3 Conducting Center Activities.....	18
5.4 Oversight and Accountability	21
6. Funding Model	23
6.1 Funding Source	23
6.2 Cost Estimates	24
7. Considerations	29
Appendix: Roadmap Task Force Members	31
References	32

FIGURES

Number	Page
ES-1. Health IT Safety Center: Achieving Safer Care through Collaboration.....	ES-2
1. Federal Health IT Strategic Principles Supporting Health IT Safety.....	3
2. Timeline of the Health IT Safety Roadmap task force Activities	5
3. Summary of Center Activities and Related Functions	14
4. Health IT Safety Center Organization Chart.....	18
5. Example Health IT Safety Center Activity Workflow	20
6. Cost Estimates for Supporting the Proposed Health IT Safety Center at Various Funding Levels.....	25

Executive Summary

The rapid pace of health IT and electronic health record (EHR) adoption in health care is yielding unprecedented benefits.¹ Today, thousands of health care professionals, hospitals, and their patients enjoy quality and safety improvements from electronic ordering, decision support, results reviewing, and other EHR functions.² At the same time, safety organizations and researchers, health IT users, and other stakeholders have found risks and hazards to patient safety associated with these systems and the complex environments in which they are implemented and used.³⁻⁵ Through a series of initiatives, the Office of the National Coordinator for Health Information Technology (ONC) identified health IT safety as an area of vital importance, requiring continual evidence, education, and engagement from health care stakeholders. ONC has worked to maximize the safety and quality of health IT while minimizing its risks. Accordingly, this roadmap details a plan for developing a proposed national Health IT Safety Center (the Center) focused on two core objectives: using health IT to make care safer, and continuously improving the safety of health IT.

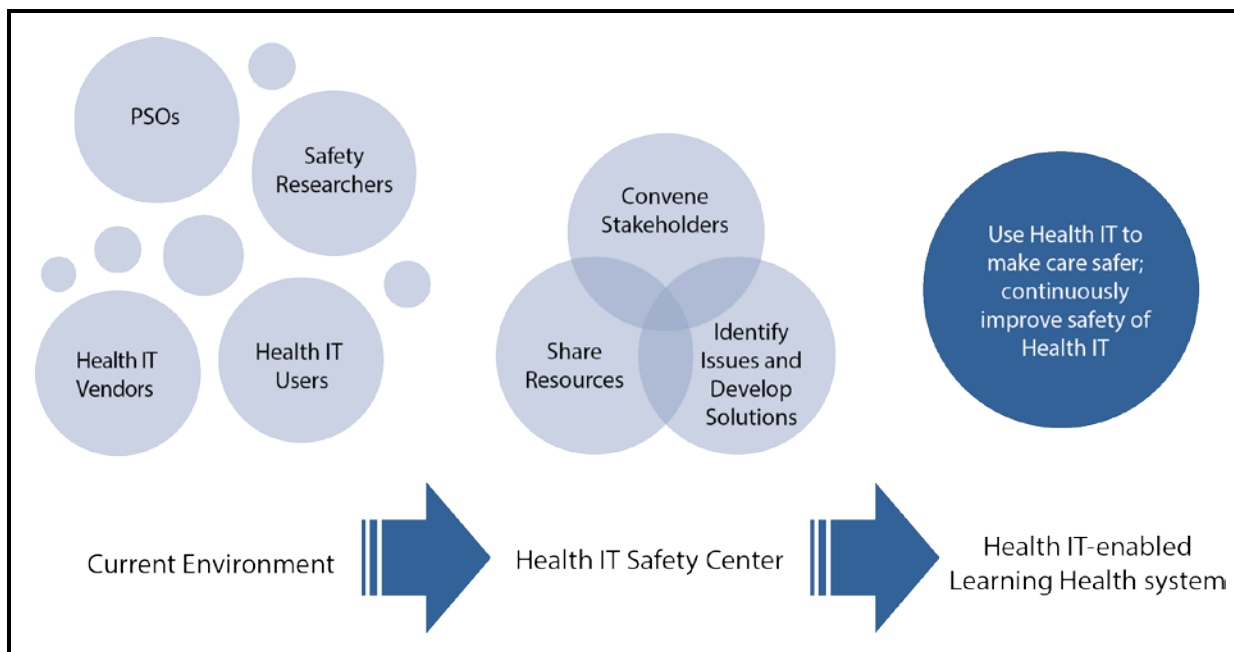
Addressing these objectives requires shared responsibility and engagement by a range of health care stakeholders (see Section 3.3). ONC contracted with RTI International to convene a task force of health IT safety experts, patient advocates, clinician users, health IT developers, health care organizations, and others to rely upon their insights in crafting this roadmap. Through a series of meetings, the task force and associated work groups provided guidance on the key areas detailed in this roadmap, including the Center's vision, objectives, and attributes as well as its core activities, operations, and funding model. Throughout their discussions, the task force identified many health IT safety-related activities that a national Center should support. Task force members repeatedly stressed the importance of having a trusted space where stakeholders could convene to review evidence and jointly develop solutions to critical health IT safety issues. This theme—*collaborate on solutions, informed by evidence*—captures the main focus of the proposed Center.

As shown in Figure ES-1, the Center would accelerate establishing a culture of safety throughout health care and a national learning system that enables health IT and its users to generate better and safer patient care outcomes.

The task force helped identify the key areas for a national Center, which include collaborating on solutions to address health IT-related safety events and hazards; improving the identification and sharing of information on health IT-related safety events and hazards; reporting on evidence on health IT safety and solutions; and promoting health IT safety education and competency of clinicians in the appropriate and safe use of health IT. Within these focus areas, task force members identified core activities (below) that evolved throughout the development of the roadmap. The Center's functions—convening,

researching, and disseminating—support core activities and inform an operating model, including staffing requirements.

Figure ES-1. Health IT Safety Center: Achieving Safer Care through Collaboration



The Center's operating model is straightforward: an executive director would lead a staff dedicated to various functions—convening, researching, and disseminating—that support proposed core activities. An advisory board, composed of Center participants and members from the private and public sectors, would represent stakeholders and oversee the executive director and staff. The Center would have a broad, active set of participants and members from public and private sectors, each contributing to and benefiting from the Center in multiple ways: providing evidence of health IT safety events, joining the Center's advisory board, participating in Center work groups and educational events, and pilot testing and adopting Center solutions. In the proposed Center, industry (including providers, patients and consumer groups, hospitals, vendors, payers, and others) and government would form a public-private partnership to convene stakeholders, identify issues, develop solutions, and further education in health IT safety.

To fund the Center, task force members supported the use of Federal seed funding, provided to a host organization through a cooperative agreement, for an initial 5-year period. Through a host organization, the Center could build on—not supplant—existing health IT safety efforts and more rapidly and effectively support Center activities using existing infrastructure. In the initial 5 years, the Center's executive director would work with the advisory board and others to develop a sustainability model to support ongoing

operations. Full cost of funding the “optimal” Center over 5 years ranges from \$17.8 to \$20.6 million (see Section 6: Funding Model). Should the Center be funded at lower than optimal levels, the roadmap’s funding model is constructed to consider the impact of decreased funding on the volume, breadth, and depth of Center activities.

The discussions among a wide variety of stakeholders and government representatives that informed this roadmap emphasized the need for action. Many stakeholders are already heavily engaged in various aspects of patient safety; the Center would support and complement these activities, not replace them. Health IT has already demonstrated that it can make care safer, although achieving its true potential for transforming health care requires all stakeholders to do much better. The safety of health IT can be improved, and the improvement should be continuous, as part of a learning health system. To realize the proposed Center—and create a trusted space for collaborating on solutions—ONC should work with stakeholders from across the health care spectrum and government to gain support for a Health IT Safety Center based on the model described in this document.

[This page intentionally left blank.]

1. INTRODUCTION

In September 2014, the Office of the National Coordinator for Health Information Technology (ONC) initiated a process to produce a roadmap to guide the development and implementation of a proposed national Health IT Safety Center (the Center). The Center was broadly envisioned as a public-private entity that would serve a trusted convener of stakeholders committed to a learning health system⁶ and engage in activities to promote the objectives of using health IT to make care safer and of continuously improving the safety of health IT. ONC contracted with RTI International to convene a task force of nationally recognized experts and health IT safety stakeholders to provide input into a roadmap that defines Center activities and how they should be executed and funded. The task force worked between December 2014 and May 2015, helping to shape the roadmap presented here, including proposed Center functions and activities, operational structure, and funding model. The **Appendix** contains a full list of Task Force members. Task force meeting summaries and a document detailing the roadmap scope are available at <http://www.healthitsafety.org>.

1.1 Background

The potential for health IT to improve patient safety has been a driving force for its adoption since the Institute of Medicine (IOM) uncovered the epidemic of avoidable harm in health care, and advocated for a redesigned health care system with health IT as part of the infrastructure for safer, better care.^{7, 8} Over a decade later, with the launch of the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs, ONC commissioned IOM to investigate and propose activities to maximize the safety and safe use of health IT and to avoid unintended consequences. The resulting report, *Health IT and Patient Safety: Building Safer Systems for Better Care (2012)*, outlined a number of recommendations. At its core, IOM emphasized that health IT safety is a *shared responsibility*. Once implemented, health IT becomes an integral part of complex, adaptive health care systems; it shapes and is shaped by a range of sociotechnical factors including people, processes, organizational policies, clinical practices, and external pressures.⁹ Accordingly, the responsibility for ensuring the safety and safe use of health IT is shared by the range of stakeholders who design, develop, implement, use, support, and benefit from these technologies. Shared responsibility requires concrete actions by these stakeholders, and, therefore, collaboration among them. Ensuring and continuously improving the safety and safe use of health IT must engage organizations and individuals with the knowledge, expertise, and ability to address safety issues, whenever they arise, throughout the lifecycle of health IT.¹⁰ IOM saw the Federal government's role as creating a framework for shared responsibility and collaboration: "The private sector must play a major role in making health IT safer, but it will need support from and close collaboration with the public sector."¹¹

Responding to the IOM report, in 2013 ONC released the Department of Health and Human Services' (HHS) *Health IT Patient Safety Action and Surveillance Plan*, which embraced the objectives of using health IT to make care safer and continuously improving the safety of health IT.¹² Since then, ONC, working with other Federal entities, has pursued strategies and activities to better understand the role of health IT in contributing to safety events and preventing them.¹³ By encouraging private sector collaboration and by funding research on the role of health IT in patient safety, Federal efforts have led to a better understanding of the need for shared responsibility among stakeholders in the private sector.¹⁴

In 2014, the Food and Drug Administration (FDA) collaborated with ONC and the Federal Communications Commission (FCC) to issue a report mandated by Congress in the Food and Drug Administration Safety and Innovation Act (FDASIA).¹⁵ The draft report provided a proposed strategy for a risk-based regulatory framework for health IT, and its recommendations are integral to the effort to establish a national Health IT Safety Center. Specifically, the draft report identified the potential creation of a Health IT Safety Center as a key nonregulatory component of an effective risk-based framework for health IT. For health IT not currently regulated by the FDA, the FDASIA draft report suggested four priorities: promote the use of quality management principles; identify, develop, and adopt standards and best practices; leverage conformity assessment tools; and create an environment of learning and continual improvement. The FDASIA draft report envisioned a Health IT Safety Center as a public-private entity that helps create a sustainable, integrated learning system for health IT safety to promote innovation and leverage and complement existing and ongoing safety initiatives.

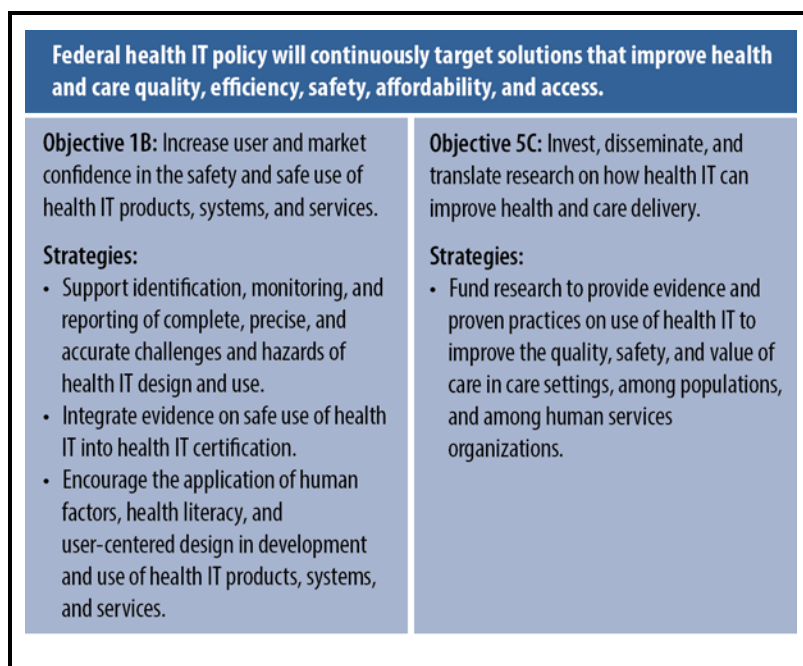
In late 2014, building on earlier work, ONC released the draft *Federal Health IT Strategic Plan*, which outlines specific goals, objectives, and strategies for achieving ONC's 5-year vision and mission.¹⁶ As shown in **Figure 1**, Federal health IT objectives include encouraging the safe use of health IT and investments supporting dissemination of evidence related to the use of health IT to improve care safety and quality.

1.2 The Need for a National Health IT Safety Center

The potential value of a national Health IT Safety Center was recognized in the FDASIA draft report, which called for a public-private entity to "serve as a trusted convener of stakeholders and as a forum for the exchange of ideas and information focused on promoting health IT as an integral part of patient safety."¹⁷ The report characterized the creation of such a collaborative effort as "critical" to reducing the need for a more regulatory approach and to strengthening a nonregulatory framework for health IT safety based in the private sector.

The need for a national Health IT Safety Center—to promote sustained cooperation and collaboration among private sector stakeholders, with appropriate Federal involvement—is also apparent in research and evidence on the role of health IT in patient safety events. Although advanced health IT has reduced adverse events¹⁸ and made care safer,¹⁹⁻²¹ health IT also contributes to adverse events²²⁻²⁶ and has failed to meet user expectations for safety-related usability.^{27, 28}

Figure 1. Federal Health IT Strategic Principles Supporting Health IT Safety



The evidence on the role of health IT in adverse events overwhelmingly confirms the importance of shared responsibility to ensure and improve health IT safety. Most recently, The Joint Commission (TJC) analyzed its sentinel event database for evidence on the role of health IT in serious patient safety events.²⁹ Problems with user interfaces, poor support for workflows and communication, and inadequate clinical content were the top factors associated with these events. TJC's research is consistent with other research including data collected by a variety of patient safety organizations (PSOs) and malpractice databases.

These health IT-related safety concerns can only be effectively addressed with collaboration, cooperation, and sharing between and among many stakeholders. Solutions to the problems identified by TJC and other research will often require health IT vendors, frontline clinician users, and health care provider organizations to work together. Support from other entities is also important. Research from PSOs, TJC, health IT vendors, medical liability insurers, academic institutions, and others has shaped understanding of the role of health IT in patient safety events. These entities need to aggregate and analyze data, but also encourage a culture where health care organizations work with vendors and other outside entities to examine root causes and identify solutions. Task force members noted, for example, that the confidentiality and nondisclosure protections offered by PSOs³⁰ were key to producing some of this research and to developing possible solutions. While task force members said that health care providers benefit from aggregating, analyzing, and learning from voluntarily reported adverse event data, research reveals the need for a range of health IT expertise in identifying health IT as a factor in these events.

The evidence supports both the recommendation in the FDASIA draft report for collaboration to address health IT safety concerns and the IOM's insight that the Federal government has an important role in fostering collaboration and sponsoring research that identifies problems and prioritizes efforts to address them.

Health IT safety problems involve a range of sociotechnical factors. Identifying safety issues, the factors involved, and their likely solutions requires multiple stakeholders to work together. Public and private stakeholders can achieve health IT safety only through shared responsibility and collaboration—this is the reason for the proposed Health IT Safety Center.

2. APPROACH TO DEVELOPING THE ROADMAP

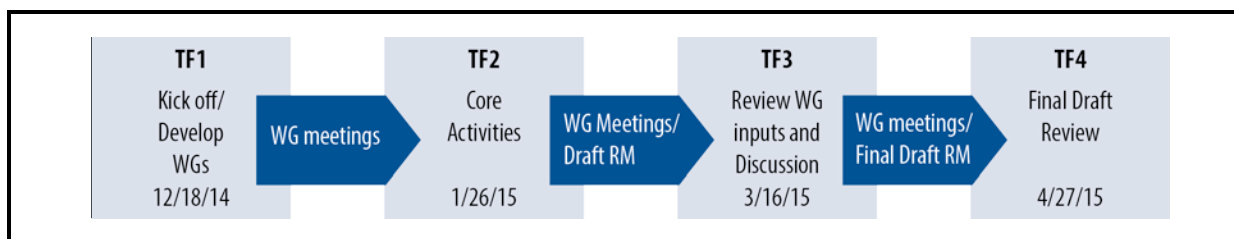
ONC asked RTI to develop a roadmap for a proposed national Health IT Safety Center, relying on input from stakeholders that would address:

1. Core activities
2. Operations and governance
3. Funding

The Health IT Safety Center roadmap process relied on input from many stakeholders engaged in health IT safety-related activities. RTI assembled a task force with representatives from national medical, hospital, and pharmaceutical associations; PSOs; patient/consumer advocacy groups; EHR developers/vendors; researchers on human factors engineering, patient safety, and health IT safety; nursing informatics; hospital IT leadership; a small provider practice; medical liability insurers; a health care accrediting organization; and a health care payer. The final task force was composed of 22 individuals representing private sector stakeholders and 5 representatives from Federal agencies: ONC, the Agency for Healthcare Research and Quality (AHRQ), FDA, the Federal Communications Committee (FCC), and the Centers for Medicare & Medicaid Services (CMS). A list of task force members and their affiliations can be found in the **Appendix**. The task force met four times between December 2014 and April 2015. Between those meetings, task force members participated in work groups to develop ideas for consideration by the full task force. While RTI is responsible for the final roadmap, the task force was asked to review and discuss a draft in April 2015. The final roadmap reflects a consensus of task force members.³¹

Figure 2 provides a general timeline of the activities undertaken by the Health IT Safety Center task force in developing this roadmap.

Figure 2. Timeline of the Health IT Safety Roadmap task force Activities



Note: task force (TF); work group (WG); roadmap (RM)

The roadmap process has operated within limitations of the potential funding agencies, ONC and AHRQ, regarding the Center's potential activities. Accordingly, inputs solicited from the task force were collected within the understanding that the Health IT Safety Center:

- Will not engage in direct investigation or surveillance.
- Will not include operating or funding the operations of a PSO.
- Will not include direct data collection.³²
- Will not include performing functions of Federal Advisory Committees.
- Will not include activities that are exclusively the responsibility of Federal entities, and, therefore, cannot be delegated to outside parties, such as the exercise of regulatory authority, establishing government programs, and decision making related to Federal budget expenditures and priorities.

3. CENTER OVERVIEW

Task force members advised on the activities, governance, and funding model for a sustainable national Health IT Safety Center. Initially, RTI worked with the task force to determine the proposed Center's vision, mission, core objectives and attributes—elements that serve as the basis of the Center. Task force members also provided inputs on the range of stakeholders that would both participate in and benefit from a national Health IT Safety Center.

3.1 Vision, Mission, and Objectives

The vision for proposed national Health IT Safety Center is simple: safer systems, better care using health IT. The Center's mission is to serve as a place where stakeholders—both individuals and organizations, in the private sector (nonprofit and for-profit) and government—work together to create a learning system committed to two main objectives:

1. Using health IT to make care safer, and
2. Continuously improving the safety of health IT.

3.2 Center Attributes

The optimal national Health IT Safety Center will have the following attributes. It will be:

Dedicated to shared learning, shared responsibility—the Center will operate as a forum for private and public sector individuals and organizations, with a common dedication to the objectives of the Center, to exchange ideas, evidence, solutions, and educational resources for using IT to make care safer and to improve the safety of health IT. Evidence and shared learning will help stakeholders clarify and understand what shared responsibility means in terms of actions and expectations.

Solutions-focused—using evidence of health IT-related safety risks and hazards, the Center's stakeholders will focus on solutions, including prioritizing areas for improvement, identifying possible solutions, pilot testing those solutions, disseminating and fostering adoption of solutions, and evaluating success.

Built upon private sector initiatives—the Center will build upon, foster, and strengthen existing and proposed initiatives in the private sector that further the proposed Center's vision, mission, and objectives.

Committed to clinical users of health IT and their patients—Center activities must support those who care directly for patients in a person and family-centered health system. Clinicians should have access to the resources needed to safely use health IT, and they should be adequately trained and supported.

A public-private partnership—the Center will provide a forum for private sector stakeholders and Federal government representatives to dialogue and work together. Initial Federal funding will launch and support Center activities, while contributions from private sector stakeholders—including in-kind staff time, facilities, and funds—will be secured over time to help support Center operations. The Center’s governance structure represents committed stakeholder groups and promotes trust, inclusiveness, and engagement.

A trusted, learning, nonpunitive environment—all activities of the Center, particularly those related to health IT safety risks and adverse events, will be conducted in a trusted space. Center stakeholders may choose to share analysis of data, examples of safety risks and adverse events, solutions, and resources—always in accordance with privacy, confidentiality, nondisclosure, and intellectual property obligations and laws.

Transparent—the operational structure of the Center strives to provide an open and transparent space to safeguard and deepen the trust of all stakeholders in the system, as well as to foster accountability.

3.3 Center Stakeholders

Although any individual or organization that shares the vision and objectives of the proposed Health IT Safety Center will be encouraged to participate, the success of the Center requires that major stakeholder groups commit to participate in Center activities, pilot projects, and governance. Representation from the following stakeholder groups should be included:

- **Patients and family caregivers and related advocacy groups.** Although patients and family caregivers must rely on others for the safety and safe use of health IT, they benefit when health IT enables high-quality, safe, and person- and family-centered care.
- **Individual health care clinicians/providers.** This category includes physicians, nurses, therapists, pharmacists, and other clinicians who bear direct responsibility for providing safe care to patients. They often work in clinical teams, in a wide range of complex care and specialty settings, and must be able to rely on the safety of health IT, as designed and implemented, to safely care for their patients.
- **Health IT developers/vendors.** In particular, EHR companies and related trade associations will be key representatives from industry. These stakeholders design, develop, and help implement and maintain their systems throughout the health IT product life cycle, and must work closely with their customers on the safety and safe use of their technology in care delivery. Often they will be their customers’ best sources of information on the safety and safe use of health IT.
- **Health care provider organizations.** These include hospitals, academic medical centers, physician group practices, long-term and post-acute care (LTPAC) organizations, pharmacies, independent labs and diagnostic imaging facilities, and other institutional health care organizations. These organizations are responsible for delivering safe, high-quality patient care, and for procuring, implementing, providing training, and supporting technologies used in this care. Provider organizations and

their associations also have an organizational and leadership structure that is responsible for programs that support the safety and safe use of health IT.

- **Health IT professionals.** These individuals within health care organizations are responsible for the safe, effective operation of health IT, including procurement, implementation, maintenance (including avoiding downtime), upgrades and modifications, privacy and security, risk management, and, often, training and safety related to its use. Health IT professionals include chief information officers (CIOs), chief medical informatics officers (CMIOs), nursing informaticists, health IT privacy and security professionals, risk managers, health information management professionals, biomedical engineers, and many other individual professionals and their associations.
- **Health IT safety researchers and educators.** This category includes academic and other researchers and educators on health IT safety, both within and outside of health care and academic institutions. They are experts in health IT safety and risk management, health IT competency, usability and human factors research, medical informatics, implementation science, and system reliability, among other disciplines.
- **Safety organizations.** This category includes AHRQ-listed PSOs and their professional associations and other organizations that provide expertise on patient safety issues, including those related to the role of health IT in patient safety. Because they are often legally separate from both health care providers and health IT developers, safety organizations can be a neutral and independent presence. PSOs also offer Federal confidentiality and nondisclosure legal protections for certain patient safety activities, such as sharing evidence of health IT safety events and conducting investigations and follow-up.
- **Accreditation organizations.** This category refers to independent, trusted third-party entities that accredit or certify health care organizations or health IT developers for compliance with standards related to the safety and safe use of health IT, including quality management, risk management, and information management standards.
- **Medical liability insurers and health insurers (payers, including self-funded employers).** Well-designed and used health IT can reduce harm and related expensive malpractice claims, unnecessary care, avoidable readmissions, and costs associated with less than optimal care. Analysis of their data and related risk mitigation or health IT improvements may enable health care organizations and health IT vendors to reduce harm and improve health IT in areas that both make care safer and reduce costs.
- **Organizations that support electronic exchange of health information and interoperability.** This category includes all types of health information exchanges (HIEs) and organizations as well as standards development organizations (SDOs) and other entities that support interoperability. Organizations that facilitate the electronic exchange of patient information and interoperability of health IT ensure that accurate, complete information is available, when needed, to provide safe care.
- **Government entities.** This category includes organizations with responsibility for patient safety and health IT. They include but are not limited to ONC, AHRQ, FDA, FCC, and CMS. State and local government representatives are also included.

[This page intentionally left blank.]

4. CENTER FOCUS AREAS, ACTIVITIES, AND CORE FUNCTIONS

4.1 Focus Areas and Activities

A set of general focus areas emerged throughout task force discussions. These represented areas of work appropriate to a national Health IT Safety Center, important to multiple stakeholders, and critical to advancing health IT safety. Within these focus areas, task force members identified various Center **activities**. Overall, the task force saw the Center as convening and facilitating interactions with health IT safety stakeholders to support the Center's main objectives.

Four focus areas help to define Center activities; these are:

1. Collaborate on solutions to address health IT safety-related events and hazards.

Task force members understood the potentially enormous benefits of health IT to make care safer and better. They also understood evidence that health IT is not as good as it should be in areas such as safety-related usability, support for clinician-clinician and clinician-patient communication and workflows, and clinical content that is accurate, complete, and useful. The stakeholders on the task force were ready to work together on solutions to problems identified by evidence. Many private and public-sector entities have already developed solutions—including best practices, guides, testing programs, educational materials and toolkits—to address known health IT-related safety risks and hazards, while others have active safety initiatives and programs. Task force members stressed the need for the Center to **support development of targeted solutions to health IT-related safety issues identified through evidence**, as well as the **dissemination, pilot testing, adoption, and evaluation of these solutions**.

Through the Center, participants would share and expand on existing solutions or work together to create new ones. Addressing problems in areas of known risk would require health IT vendors and health care organizations to work together based on their expertise and on who can best control or mitigate risks of these problems. The Center would convene and facilitate work among health IT vendors, providers, and others in creating effective, evidence-based solutions. To ensure improvements in health IT safety, task force members advocated that the Center develop implementation specifications and guidance related to these solutions; test solutions and their implementation materials in real-world settings; actively promote and support their dissemination; and evaluate their effectiveness once implemented.

2. Improve identification and sharing of information on health IT-related safety events and hazards.

In order to prioritize collaboration on solutions, the Center will require evidence showing how health IT plays a role in adverse events and hazards. The task force members emphasized the value of analysis and aggregation of adverse event data across many organizations, which is greatly facilitated by standardized reporting and

classification. Task force members identified a number of methods to identify, categorize, and analyze safety events and hazards, many of which have not been validated and vary in their ability to capture useful data on health IT accurately.

Today, adverse event reporting relies on voluntary reporting by providers and retrospective analysis of events. Many providers use the AHRQ Common Formats (CFs) to voluntarily report adverse events to PSOs, often augmented by other standardized or nonstandardized reporting formats. Task force members discussed the limitations of the CFs in reporting on health IT as a contributing factor in events. AHRQ, however, has a process for improving the CFs. As one Center activity, participants may use their experiences to provide suggestions to AHRQ about how CFs and other frameworks may be strengthened over time to better capture health IT-related events. Task force members supported improving the existing CF framework for reporting. More broadly, they supported **strengthening and augmenting existing ways to identify and classify health IT-related safety events**. They also advocated that the Center **identify ways to encourage better reporting of health IT-related events** by improved training, easier reporting mechanisms that are better integrated into workflows, and reduction of other barriers to reporting.

Task force members also emphasized using multiple data sources in addition to PSO data—specifically medical malpractice liability claims, sentinel events, public safety event databases, and even IT help desk tickets—to identify and characterize health IT safety related risks and hazards. If such diverse data sources can be used to identify the role of health IT in safety events using common classification schemes, our ability to understand problems and make improvements will be enhanced. Task force members noted that the results of analyses of these data would need to be shared voluntarily with the Center, subject to any organizational obligations and limitations on use.

Task force members also stressed the need for the industry to consider tools that allow for automated detection, identification, and reporting of safety issues. Recognized methods include “trigger tools” run on information in EHRs³³ to identify adverse events and EHR computerized point of entry (CPOE) evaluation tools or “flight simulators” also run on EHRs to improve detection of potential adverse events.³⁴ Such tools have demonstrated great promise.^{35, 36} Accordingly, task force members believed the Center would support activities that **identify and share advances in automated safety tools for adverse event detection and health IT-related safety improvements**.

3. Report evidence on health IT-related safety and on solutions. Every year significant research is reported related to health IT and patient safety, and solutions are developed in the private sector and by government. The Health IT Safety Center should build on that base, learn from it, and help disseminate more rapidly and broadly information on health IT-related safety and solutions.

Task force members thought the Center should **produce reports summarizing current evidence of health IT safety** from a broad range of sources, including PSOs, medical liability insurers, academic researchers, EHR vendors, provider organizations, accreditors, and others. This activity would expand the knowledge base about health IT safety events and hazards, root causes, and strategies and solutions that optimize the safety and safe use of health IT.

Task force members also anticipated the need for additional, focused research and analysis in areas of concern identified by stakeholders or stemming from specific events or reports. In special reports or information briefs, the Center would present **targeted examinations of specific issues**—such as safety-related concerns in EHR user interfaces and usability—and **identify approaches to addressing these issues**. These efforts would ultimately support Center participants in developing and adopting actionable solutions to health IT safety risks and hazards.

Task force members identified organizations, such as PSOs, that are actively working with providers and, in some cases, vendors to develop best practices and solutions to health IT safety issues. The task force members recommended that the Center **serve as a clearinghouse for health IT safety solutions, evidence reports, and best practices**.

4. Promote health IT-related safety education and competency. Task force members cited a range of existing health IT safety educational resources, including Webinars, online courses and training modules, guides, presentations, and reports. As with health IT-related safety solutions, these educational resources are dispersed across the health care system; no single repository exists. The Center will build upon and foster such activities. Task force members thought that the Center should **serve as a clearinghouse for health IT safety educational resources** by maintaining a central Web-based directory, well-organized and searchable, frequently updated and open to the public.

Task force members also identified the potential need to **develop new educational resources and training materials to build health IT-related competencies** in designing and implementing safer health IT and in using health IT safely. Such work would be in priority areas identified by the Center that are not being addressed by others.

4.2 Core Functions

Across these focus areas, RTI identified core Health IT Safety Center functions that would inform Center operations and staffing. These general processes are critical to helping the Center achieve its objectives and conduct its activities (summarized in **Figure 3**). Core functions include:

















Convening—The task force agreed that the Center’s main function should be to assemble stakeholders to find solutions in high-priority health IT safety areas. Convening means assembling stakeholders both in person and virtually to share existing

analyses of health IT safety event data, agree upon high-priority issues, identify or develop solutions, test and evaluate them, and engage in education and training.

Researching—This function supports and informs the development of solutions to high-priority health IT safety issues. First, research means collecting and assessing existing analyses of health IT safety event data to identify issues and gaps. It also means identifying and, as needed, supporting development of best practices, tools, interventions, and educational resources to prevent or address health IT safety issues. Research consists of identifying current methods to characterize health IT-related safety events and hazards, and assessing where these may be extended or improved. Finally, this function includes evaluating the impact health IT safety solutions and educational efforts, focusing on their effects in reducing health IT safety risks and hazards. Evaluation also includes assessing effectiveness of educational and training resources on health IT competency. The Center would use assessment and evaluation findings to refine or improve Center work products such as evidence reports and solutions.

Disseminating—Activities related to this function include promotion and distribution of Center work products—including new methods, evidence reports, solutions, and educational materials—to Center stakeholders. Dissemination would also support real-world pilot testing, implementation, and evaluation of health IT safety solutions across different care settings. An important means of dissemination includes a Web-based directory of health IT safety resources developed by members and participants and vetted by the Center staff.

Figure 3. Summary of Center Activities and Related Functions

Proposed Health IT Safety Center Activities	Convening	Research	Dissemination
Support development of targeted solutions to health IT-related safety issues identified through evidence			
Dissemination, pilot testing, adoption, and evaluation of solutions			
Strengthen and augment existing ways to identify and classify health IT-related safety events			
Identify ways to encourage better reporting of health IT-related events			
Identify and share advances in automated safety tools for adverse event detection and health IT-related safety improvements			
Produce reports summarizing current evidence of health IT safety			
Targeted examinations of specific issues and identify approaches to addressing issues			
Serve as a clearinghouse for health IT safety solutions, evidence reports, and best practices			
Develop new educational resources and training materials to build health IT-related competencies			

5. OPERATIONS

This section describes how a national Health IT Safety Center would operate. It discusses Center funding agencies and a host organization; proposed Center participants and members; and Center staff and their associated roles and responsibilities. This section also features an example of how the Center participants, members, and staff would work together across core functions and activities, and discusses Center oversight and governance.

5.1 Operations Overview

Operationally, the Center must support stakeholder collaboration around the activities and functions identified above in a public-private entity. The Center would not be housed within a government agency. However, in keeping with the FDASIA draft report and the government's interests, obligations, and authorities, one or more Federal agencies would serve as a **funding agency** to provide initial seed funding and guidance for the Center through a cooperative agreement.

The staff and activities that constitute the work of the Center would, at least initially, operate as a program within a single, existing **host organization** that would be able to enter into a cooperative agreement with the funding agency. Any candidate host organization would need to have patient safety and health IT expertise and an operational structure that could support the staffing model described below. The host organization must also have a mission that encompasses the vision, mission, objectives, and activities of the proposed Center. Most of the Center's activities would be conducted virtually, with exceptions for important meetings and events. The Center would be a physical place, however, and not a virtual entity whose entire staff is geographically dispersed. Accordingly, the entity hosting the Center would provide core infrastructure—including facilities as well as telecommunications and administrative staff—to support Center operations. The host must be able to accept charitable contributions that it could use to support Center activities, above and beyond those provided through the cooperative agreement. The host organization must also be able to oversee Center activities and staff, while accommodating an **advisory board** of stakeholders who direct and prioritize Center activities, subject to any terms of the funding agreement and the legal oversight obligations of the host organization. At some point in the future, the Center could be spun out of the host organization. However, as the Center would aim to build on current efforts, and as many organizations exist that have the attributes described above, the Center would initially be based in a host organization.

The Center would be inclusive—open to anyone interested in health IT safety and who could benefit from Center activities. Center participants would interact with one another and with Center staff through various means to participate in the Center's activities and core

functions. The Center would have a limited number of dedicated staff to facilitate and manage Center activities. Oversight of the Center would vary depending upon the funding agency and host organization's responsibilities and obligations, but the goals of any oversight body would be consistent: to ensure the appropriate use of Center resources in meeting its objectives, and to help assess progress towards those objectives.

5.2 Center Roles and Responsibilities

As a public-private partnership, the optimal Center would include broad participation from a range of stakeholders. **Center participants** would include individuals and organizations with an interest in health IT safety. Participants would be able to provide input into the Center's activities, receive work products (including evidence reports and solutions), and participate in education and training sessions. Center participants would likely be those individuals or organizations from various Center stakeholders described in section 3.3, but anyone could participate.

Center members would constitute a large subset of participants, the main difference being the level of commitment to engage in Center activities. Participation in the Center would be free and open to everyone. Members would be expected, however, to contribute to the Center in several ways, foremost by identifying areas of common interest to work on together. They would agree to share evidence and analyses (de-identified of patient information) of health IT safety events and offer solutions (practices and tools) developed in addressing those events. Center members may also be asked to provide in-kind contributions and funds to support Center activities; membership in the Center's initial years would generally not be contingent upon a participant's ability to provide any contributions, however.

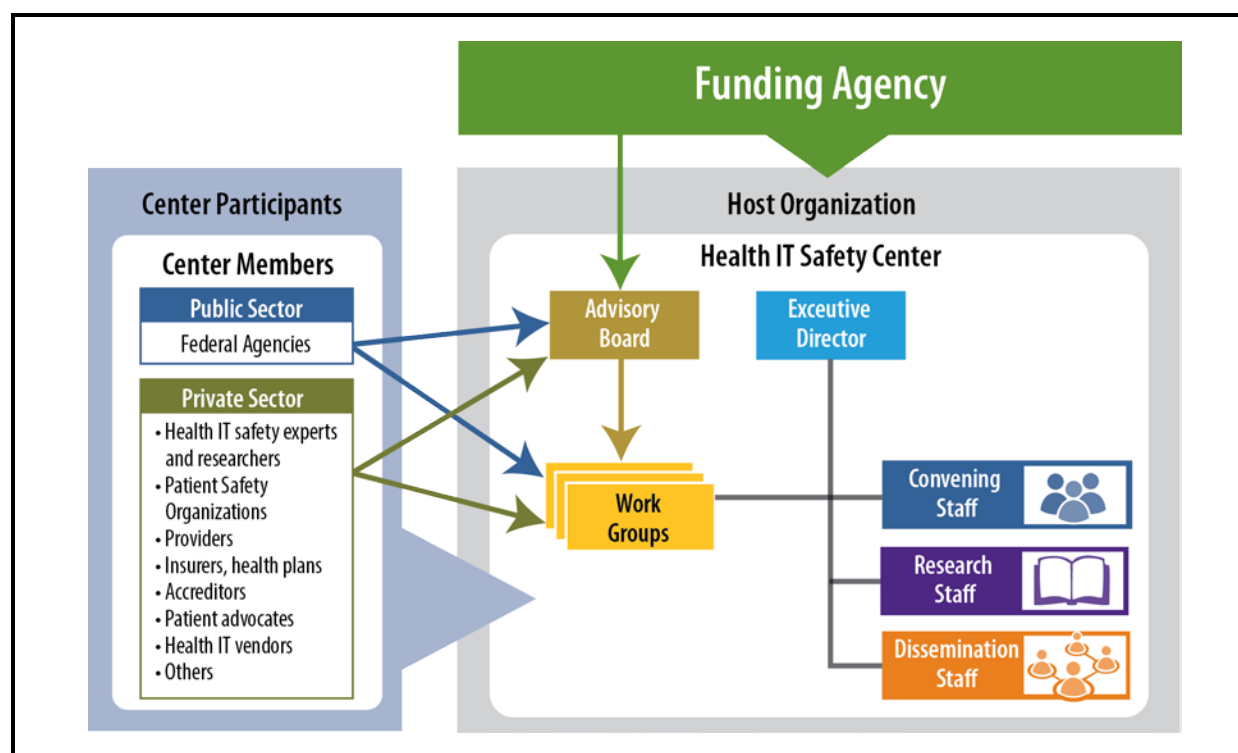
The Center would be led by an **executive director**, selected by the host organization after consulting with the funding agency. The executive director would engage the advisory board in planning for Center activities; oversee the Center's launch and day-to-day operations; develop and execute a Center work plan; develop Center operating policies and procedures; manage Center staff; identify additional funding sources; and secure and sustain engagement by Center members and participants.

Initially, the Center staff would consist of **convening staff** who would focus on development functions—including activities around review of evidence, solution identification and development, and education. These staff would support the convening and management of Center work groups, described below. Center staff would also include **research** staff who would support research and analysis—including work on methods, producing evidence reports, and support for solution development, and **dissemination staff** who would promote and distribute Center work products—including evidence reports, solutions, educational and training resources, as well as assist with the implementation and

evaluation of Center work products. Dissemination staff would also help develop and support the Center’s Web-based clearinghouse of health IT safety-related activities, research, and resources.

With input from the funding agency, the host organization would initially³⁷ select the executive director and appoint individuals representing major stakeholders to serve on the initial governing body for the Center—the Center’s **advisory board**. Once convened, this advisory board would direct and prioritize Center activities and advise the executive director on work important to the Center’s launch and operation. The advisory board would work with the executive director to develop and execute a work plan, review Center work products (e.g., summary reports on the evidence of health IT safety) prior to their release, and provide oversight related to the Center’s operations—including the development of policies and procedures. The advisory board would also identify additional stakeholder organizations to approach for joining the Center as members and work with the Center director and convening staff on recruiting new members and retaining current ones.

Finally, the Center would rely on **work groups** to develop solutions and work on projects prioritized by the advisory board. Work groups would be composed of Center members and participants, advisory board members, and other experts, and supported by the convening staff. Examples might include a work group targeting development or refinement of methods to identify health IT safety events and hazards, or one focused on development of a solution related to a health IT safety risk. Over time, work groups may become more permanent for enduring facets of work in key areas, such as usability, system design and system implementation. With support and input from research and convening staff, work groups would produce work products (e.g., solutions, educational resources) for final review and approval/endorsement by the Center advisory board and executive director. See **Figure 4** for an illustration of the organization of the Health IT Safety Center.

Figure 4. Health IT Safety Center Organization Chart

5.3 Conducting Center Activities

The Center staff aligns with the Center's core functions. Generally, convening staff will help the Center director work with the advisory board and support the work groups in development of best practices, tools, and other solutions related to health IT safety; research staff will focus on identification, analyses, and evaluation functions;; and the dissemination staff will support dissemination and education functions. In practice, however, these staff members will need to work with one another, with Center participants and members, the advisory board, and the executive director to complete Center activities. To illustrate how these entities would work together, we describe a general scenario below of how core functions—from research to convening to dissemination—would operate under the proposed Health IT Safety Center.

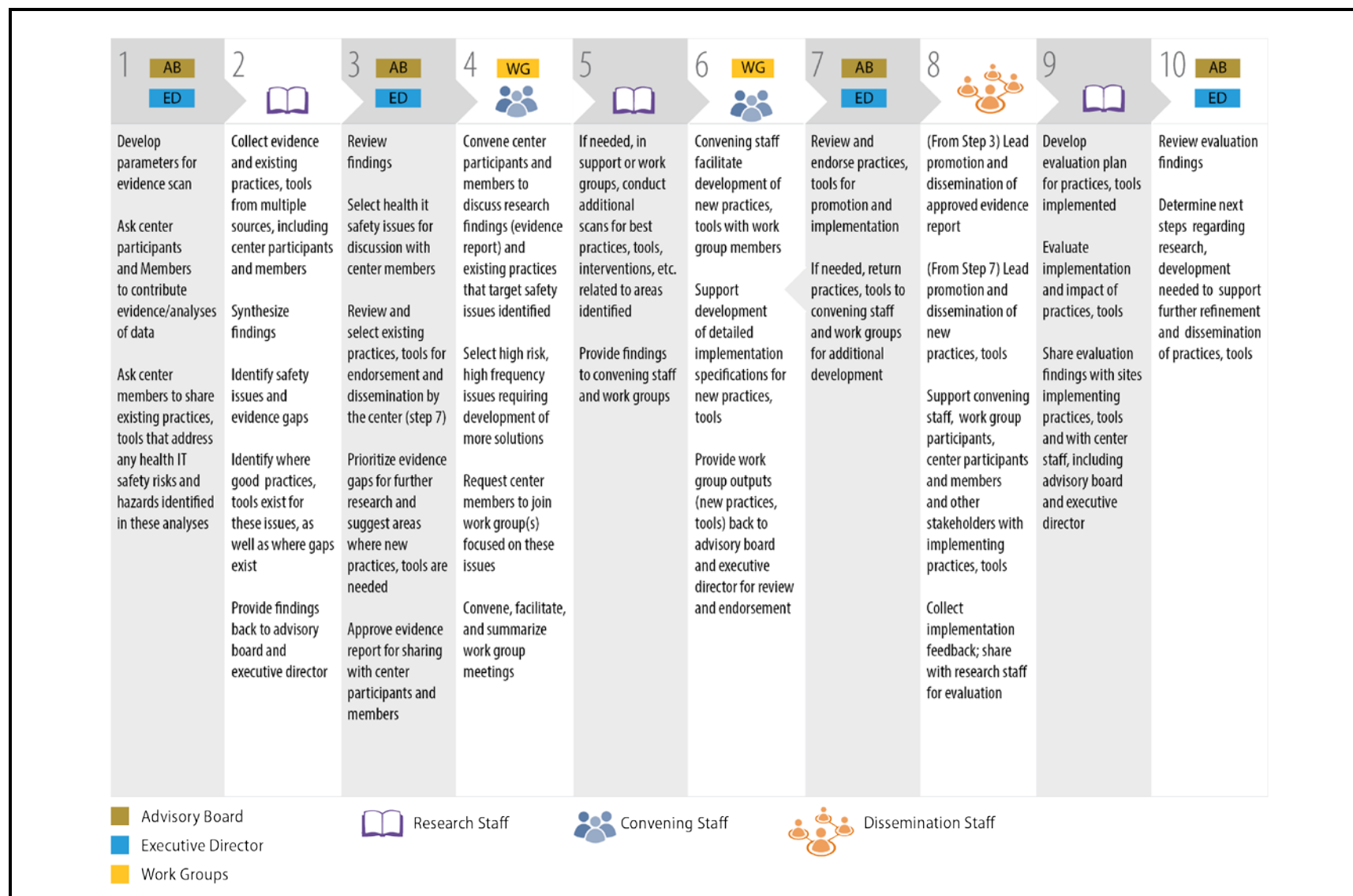
To support shared learning around health IT safety, one of the Center's first activities will be to develop an ongoing process for collecting, analyzing, and synthesizing evidence on health IT-related safety events and hazards³⁸ and on related solutions. The Center should develop this process to ensure it may be replicated annually and used to evaluate progress and new areas of concern.

The Center's research staff would search the peer-reviewed literature and request existing analyses of health IT safety event data from Center participants, members, and other health

IT stakeholders. Research staff would compile these sources, assess them, sort them into a framework, and then report back to the advisory board and executive director. Using this report, the advisory board and executive director would help determine candidate topics for review and discussion with Center members as well as to identify gaps requiring further research. Specific criteria—such as high-risk, high-frequency safety events—would be identified and guide topic selection. The Center’s convening staff would then bring candidate topics to Center members for discussion and for creating work groups focused on developing solutions to the health IT safety risks and events identified. To support these work groups, the research staff would conduct additional, targeted research for additional evidence, best practices, tools, and interventions related to these health IT safety issues. The gaps identified from the initial broad scan would be used to further inform the Center’s research agenda to support more in-depth research. Depending upon research focus and scope, the Center would work with other organizations or researchers to complete more targeted research and analyses. **Figure 5** summarizes the 10 steps that would be included in this example.

With the most current and complete evidence at hand, the convening staff would facilitate the development of new practices and tools with work group members that address the issues identified. As part of this development, the work group, supported by research staff, would also create detailed implementation specifications for these new practices and tools. When development is completed, the convening or research staff would provide work group outputs (new practices, tools) to the advisory board and executive director who would review and approve them for proof of concept testing, pilot testing, dissemination, or other appropriate follow-up. The dissemination staff would then lead the promotion and dissemination of these resources to key audiences. The dissemination staff would also support convening staff, work group participants, Center members, and other stakeholders with implementing practices, tools, and with collecting implementation feedback to share with research staff for evaluation. In parallel with dissemination, the research staff would develop an evaluation plan for the new resources and then evaluate the successes and challenges with their implementation as well as their impact on health IT safety. When evaluation findings are completed, the research staff would share them with sites implementing practices and tools and with Center staff, including the advisory board and executive director. Finally, the advisory board and executive director would review evaluation findings and determine next steps regarding additional research or development needed to support further refinement and dissemination of these new resources.

Figure 5. Example Health IT Safety Center Activity Workflow



This example depicts a series of steps across several proposed Center functions and activities and the roles and responsibilities of Center staff and Center members in these functions. Other organizations have followed similar processes related to solving patient safety problems. The callout box on this page provides an example of how health care stakeholders worked together to address a critical patient safety issue—wrong-site surgery—further illuminating how the Center would operate.

As part of launching the Health

IT Safety Center, the executive director will develop a more complete operational plan that outlines the steps, participants, inputs, and outputs for other Center functions and activities, starting with the higher and working to lower priority activities.

Wrong-Site Surgery

Solving serious safety problems that happen infrequently is difficult at any given organization because no one person or organization sees enough cases to detect broad patterns. The Health IT Safety Center can serve an important role in preventing low-frequency but high-severity events in which the stakes are high but the causes are poorly understood.

A case in point is the Pennsylvania Patient Safety Authority's experience with wrong-site surgery. Through its detailed analysis of hundreds of cases, the Authority developed the evidence base on practices that were effective in preventing wrong-site surgery. They developed principles for prevention, tools to implement safer practices, and a collaborative learning model to encourage diffusion of the prevention strategies. As a result of its efforts, the efforts of the provider organizations involved, as well as others contributing to this field, the incidence of this type of adverse event has been substantially reduced.

5.4 Oversight and Accountability

Providing oversight and ensuring accountability are central to effective governance. Center oversight would, in part, be provided by the host organization in accordance with the terms of the cooperative agreement. The Center's advisory board would also provide governance, operating within the constraints of the host organization and cooperative agreement. The advisory board would guide the executive director regarding Center activities and priorities, and help oversee execution of the Center's operational plan.

To support operations as described—including the necessary staff and infrastructure—requires funding. Section 6 outlines a funding model based on an initial cooperative agreement that supports these operations at various levels, and details a phased approach over 5 years to launch, establish, and sustain the Center.

[This page intentionally left blank.]

6. FUNDING MODEL

In developing a funding model for the proposed Center, we considered two main components: funding source and cost estimates. The funding source identifies the main entity and mechanism for supplying seed funding for the first 5 years of Center operations. For the cost estimates, ONC instructed RTI to estimate funds needed to operate an “optimal” Center, and how Center operations and activities would be affected at 75, 50, and 25 percent of optimal funding levels. Accordingly, we also review cost estimates that detail 4 levels of Center funding for 100, 75, 50, and 25 percent of the optimal Center.

6.1 Funding Source

Initial funding from the Federal government—such as ONC or AHRQ—through a cooperative agreement would ensure that the Center accomplishes a public purpose, while also ensuring that the many different stakeholder organizations are equally encouraged to engage in Center activities and governance. However, stakeholders must benefit from engagement with the Center. If the Center’s initial activities and outputs advance health IT safety and meet stakeholder’s needs, Center members may be willing to support some or all of the Center’s operating costs.

Host Organization Criteria	
<ul style="list-style-type: none">• Ability to enter into a cooperative agreement with the funding agency• Patient safety and health IT expertise; history of involvement with patient safety initiatives• Mission that encompasses proposed Center vision, objectives, activities, etc.• Operational capacity and infrastructure to support Center staffing model and proposed activities• Ability to maintain neutrality between a diverse set of stakeholders• 501(c)3 status and ability to receive tax-free financial contributions• Ability to receive additional grant and contract funds• No conflicts of interest relative to Center activities and work products (solutions)	<p>The host organization receiving the cooperative agreement would operate the Center for an initial 5-year period, with plans for an evaluation of operations in year 3 as part of developing a sustainability model for ongoing operations when seed funding expires after year 5.</p> <p>It is envisioned that non-Federal funding from participants, members, and other supporters would begin to flow into the Center in year 3 and reach a steady state in year 5.</p> <p>The proposed funding source—a cooperative agreement awarded through open competition to a host organization—has several advantages. As a single source of funds, this agreement would allow relatively rapid launch of the Center. A cooperative</p>

agreement supports more direct agency involvement in Center operations and activities than grants, while offering more flexibility than contracting mechanisms. Further, relying on

a host organization follows one of the Center’s main attributes—to build on and strengthen the private sector—by using the facilities and operating structures of a preexisting host organization rather than bearing the costs of creating a new entity. Several organizations already working in health IT safety would meet host organization criteria, thus further ensuring more rapid Center launch.

6.2 Cost Estimates

RTI developed Health IT Safety Center cost estimates using assumptions about the staff needed to support the functions of the Center, the level of effort for those staff, and other direct costs needed to support Center operations and activities. To estimate costs for each staff, we used labor rates from the Bureau of Labor Statistics, May 2014 National Occupational Employment and Wage Estimates.³⁹ We also assumed that the time contribution by Center participants and members would be voluntary, in-kind support, not funded by the Center. An estimated funding range is provided for each level, which accounts for variability in the operational and overhead costs and geographic location of the host organization.




The cost model estimates the complete cost to support the activities of the Center as described at each funding level, regardless of funding source. However, as the description of the roles and responsibilities indicate, we have proposed activities related to funding sustainability. Specifically, Center staff will investigate additional forms of funding in accordance with a three-phase rollout for Center operations over 5 years as follows:

- **Phase 1: Year 1 – Start-Up.** Federal seed funding is initiated through a cooperative agreement to the host organization. In-kind support comes from Center participants and members.
- **Phase 2: Years 2-3 – Establishment.** Federal funding and in-kind support continue. Financial support from other sources initiated Center staff allocated to developing options for sustainability.
- **Phase 3: Years 4-5 – Sustainability.** Federal funds taper off. Other funding sources are initiated and increased.

Estimated funding for the **optimal** Center includes the staffing and support costs needed to execute Center activities identified above. The capabilities of the Center staff and their familiarity with the landscape of health IT safety will be essential to the success of the Center. Other costs associated with Center operations include those for supporting a Center website, teleconferencing and Web conferencing, travel, producing printed materials, and shipping. The funding model includes funds to retain subject matter experts, which could be used in research, tool, and educational resource development, and consultation around best practices.

Figure 6 provides a list of staff, other costs, and activities for each funding level. The breakdown of staff and full-time equivalent for each staff position to support operations at varying funding levels is provided. At the optimal level, the executive director and three functional area managers provide full-time support for their respective activities. The Center leadership is assisted by technical and administrative staff to support Center activities at different funding levels. These include project managers, project coordinator/executive assistants, professional editorial and graphic artists, Web and database programmers, meeting planners, and financial analysts for fiscal monitoring.

Figure 6. Cost Estimates for Supporting the Proposed Health IT Safety Center at Various Funding Levels

		Optimal (100%)	Functional (75%)	Lower Impact (50%)	Not Recommended (25%)
Staff	Executive Director	Full time (1.0 FTE)	Full time (1.0 FTE)	Full time (1.0 FTE)	Full time (1.0 FTE)
	Research Lead	Full time (1.0 FTE)	Full time (1.0 FTE)	Part time (.75 FTE)	Part time (.5 FTE)
	Research Staff	2 Full time (2.0 FTE)	1 Full time (1.0 FTE)	1 Part time (.3 FTE)	NONE
	Convening Lead	Full time (1.0 FTE)	Full time (1.0 FTE)	Full time (1.0 FTE)	Full time (1.0 FTE)
	Convening Staff	2 Full time (2.0 FTE)	1 Full time (1.0 FTE)	1 Part time (.5 FTE)	NONE
	Dissemination Lead	Full time (1.0 FTE)	Full time (1.0 FTE)	Full time (1.0 FTE)	Part time (.5 FTE)
	Dissemination Staff	2 Full time (2.0 FTE)	1 Full time (1.0 FTE)	1 Part time (.5 FTE)	NONE
	Administrative Staff	2 Full time, 5 Part time (2.5 FTEs)	7 Part time (1.7 FTEs)	4 Part time (.75 FTEs)	3 Part time (.4 FTEs)
	Sustainability Assessment	2 Part time (0.6 FTEs)	2 Part time (0.6 FTEs)	2 Part time (0.4 FTEs)	2 Part time (0.25 FTEs)
Operations	Convene 	Establish and Convene Advisory Board	Establish and Convene Advisory Board	Establish and Convene Advisory Board	Establish and Convene Advisory Board
		Convene 4 Work Groups	Convene 3 Work Groups	Convene 2 Work Groups	Convene 1-2 Work Groups
		Develop 4 solutions	Develop 3 solutions	Develop 2 solutions	Develop 1-2 solutions
	Research 	Annual evidence scan and report	Annual evidence scan and report	Annual evidence scan and report	Annual evidence scan and report
		Conduct targeted research on 4 topics	Conduct targeted research on 3 topics	Conduct targeted research on 2 topics	Conduct targeted research on 1-2 topics
		Coordinate pilot implementations of 4 solutions	Coordinate pilot implementations of 3 solutions	Coordinate pilot implementations of 2 solutions	Coordinate pilot implementations of 1-2 solutions
	Disseminate 	Evaluate outcomes	Evaluate outcomes	Evaluate outcomes	Evaluate outcomes
		Market & disseminate 4 solutions	Market & disseminate 3 solutions	Market & disseminate 2 solutions	Market & disseminate 1-2 solutions
		Create and maintain Web-based directory of health IT safety resources	Create and maintain Web-based directory of health IT safety resources	Create and maintain Web-based directory of health IT safety resources	Develop basic/static Web-based listing of health IT safety resources
Other Costs	Computer and other IT	Computer and Network services Telephone/ Web Conferencing	Computer and Network services Telephone/Web Conferencing	Computer and Network services Telephone/Web Conferencing	Computer and Network services Telephone/Web Conferencing
	Travel	Support for individual trips and high-priority group in-person meetings	Support for individual trips and 1 group in-person meeting	Support for individual travel	NONE
	Subject Matter Expert funds	\$1M/yr	\$600K/yr	\$300K/yr	NONE

All activities in the optimal model are considered high priority, including funds to retain subject matter experts to assist with development of solutions to identified problems. Input from the task force also stressed the importance of including limited travel funds to support in-person meetings. These funds would be used to convene, for example, Center staff and

advisory board members to discuss critical, complex, and sensitive issues. In years 3 and 5 after Center launch, we include a part-time evaluation specialist and a part-time economist to assess Center performance and help develop options for sustainability. The estimated funding required to support the optimal Center is between \$17.8 and \$20.6M total for 5 years.

To develop cost estimates for lower funding models, RTI asked task force members to prioritize the activities that would provide the highest impact in the event that full funding for the optimal model was not available. At the 75 percent of optimal funding level, the majority of task force members felt that the Center should retain all activities, but reduce their volume and scope. This model provides **functional** support for convening, research, and dissemination and retains a full-time executive director and full-time support for the leadership of each functional area. The amount of technical and administrative support is reduced, in conjunction with the reduction in volume of each activity. In addition, travel funding is reduced, and subject matter support is decreased by 40 percent from the optimal model. The estimated funding required to support a functional Center is between \$12.9 and \$14.9M total for 5 years.

At the 50 percent of optimal funding level, support for all three major functional areas is retained, but the volume of activities under each is further reduced, thus making the work of the proposed Center **lower impact**. More focus is given to convening and dissemination activities at this funding level, with significant reductions in the activities and support for research leadership and staff. Task force members felt that the work of the Center at this level would still be valuable because it would fill essential gaps related to convening disparate stakeholder groups. At this level, the executive director and advisory board would be charged with identifying only the areas of highest need or most immediate concern. Center staff would continue to support work groups to share knowledge, identify solutions, and disseminate findings in these critical areas, but would not have time to support topics that may be less urgent or lower priority. Funds to support a funding sustainability review in years 3 and 5 would be cut, which will result in a less detailed and actionable report. Travel funds are also cut significantly. Funds to include subject matter experts to help support solution-development is reduced by 70 percent from the optimal level. The estimated funding required to support a low-impact Center is between \$9.1 and \$10.5M total for 5 years.

Finally, at 25 percent of optimal funding, only the executive director and convening function lead would be full-time staff members. Staff to lead both research and dissemination activities would have only part-time support. Technical staff to support activities in the three functional areas would be removed completely, and administrative support staff is minimal. In line with input from the task force, this model retains the basic convening functions, as these are the most valuable provided by the Center. This funding level does not contain support for a strategic communication plan, education or engagement activities, travel, or

any funds to retain subject matter experts. Support for staff to conduct a funding sustainability review in years 3 and 5 has been cut to include a general overview only. The estimated funding required to support a Center is between \$5.1 and \$5.9M total for 5 years. However, task force members stressed that this model was **not recommended**. They did not view it as a viable operational model for achieving any measurable impact on improvements in the knowledge or culture around health IT safety.

[This page intentionally left blank.]

7. CONSIDERATIONS

This roadmap details an approach to creating a national Health IT Safety Center. It outlines the Center's vision, mission, objectives, and attributes; describes its core activities; proposes operating and governance mechanisms; and offers a funding model to support the first 5 years of Center operation. In determining how to act upon the guidance in this document, ONC and other Federal and industry stakeholders should consider the following points.

The Center described in this roadmap does not propose to cover all potential Center activities—only those that the majority of task force members thought would be of greatest value to stakeholders currently and that are within ONC and AHRQ's current authorities. In this regard, the roadmap serves as a starting point for a national Center. Task force members anticipate that the Center would evolve, with varying emphasis on certain activities year to year, and new activities added—or irrelevant/redundant activities removed—over time.

Most of the activities and examples of proposed Center processes in this roadmap focus on one of the Center's two main objectives: continuously improving the safety of health IT. Though not discussed in detail, the same core functions (convening, researching, and disseminating) and Center operational processes and staff would be applied to the other main objective: using health IT to make care safer. The initial focus on improving safety stems from the task force member's shared responsibility for health IT safety. The Center as envisioned, however, would also aggregate existing analyses of where health IT improves quality and safety, and convene participants and members to determine how best to share these improvements and measure their impact across the health care system.

Many health IT safety stakeholders, including task force members, already engage in one or more of the Center's proposed core activities. Task force members noted that a single means to convene all public and private sector stakeholders and to effectively aggregate and curate a range of resources is currently lacking. The Center's role as a convener was of high value to task force members. As ONC and others consider the funding levels outlined in Section 6, supporting the Center's ability to convene stakeholders for development of solutions should be paramount. The funding model assumptions and cost estimates reflect this emphasis.

While offering some Federal support to the development of health IT safety evidence and solutions, the lowest level of Center funding (25 percent) would not measurably advance health IT safety. Task force members questioned the value of funding a Center that could not produce more in the way of support than, for example, convening one work group and developing one solution for a health IT safety-related issue.

Task force members noted the importance of developing a culture of safety in their own organizations, and the Center's role in fostering safety cultures. Organizations with strong safety cultures have dedicated safety programs. With enough funding and participation, the Center activities, then, could support inclusion of health IT safety as a key component in any patient safety program.

Finally, the roadmap development process created more than this document. Through their participation on the task force, stakeholders from major provider organizations, health IT vendors, researchers and PSOs, and safety advocates developed relationships and fostered a shared commitment to improving health IT safety. By supporting more immediate implementation of this roadmap, ONC and other Federal entities will be able to build on these relationships and increase the likelihood of improving safety and quality through a public-private partnership.

Appendix: Roadmap Task Force Members

Terry Fairbanks, MD, MS

Director, National Center for Human Factors in Healthcare and MedStar SITEM, MedStar Health

Peggy Binzer

Executive Director, Alliance for Quality Improvement and Patient Safety

Richard Landen, MBA, MPH

Director of Regulatory Affairs, QuadraMed
Representing the HIMSS Electronic Health Record (EHR) Association

Ronni Solomon, JD

Executive Vice President and General Counsel, ECRI Institute

Dean F. Sittig, PhD (Alt: Hardeep Singh, MD, MPH)

School of Biomedical Informatics, University of Texas Health Science Center, Houston, TX

Tejal Gandhi, MD, MPH

National Patient Safety Foundation

Rebecca P. Snead, BSPHarm

National Alliance of State Pharmacy Associations, Alliance for Patient Medication Safety

Steven Stack, MD

President-elect, American Medical Association

Diane Jones, JD

American Hospital Association

David Classen, MD

CMIO, Pascal Metrics; Associate Professor of Medicine, University of Utah

Gerard M. Castro, PhD, MPH

Project Director, Patient Safety Initiatives; Office of Patient Safety, The Joint Commission

Luke Sato, MD

Senior Vice President and Chief Medical Officer, CRICO/Risk Management Foundation

Susan McBride, PhD, RN-BC, CPHIMS

Professor, Texas Tech University Health Sciences Center, School of Nursing

Shafiq Rab, MD

Hackensack University Medical Center
Representing College of Healthcare Information Management Executives (CHIME)

Eugene Heslin, MD

Bridge Street Medical Group

Stephanie Zaremba, JD

athenahealth

Missy Danforth

Senior Director, Hospital Ratings, The Leapfrog Group

Michael Cohen, MD

Professor, Department of Pathology, University of Utah

Emily Barey RN, MSN (Alt: Jim Russell)

Director of Nursing Informatics, EPIC

David B. Troxel, MD

Medical Director and Secretary, Board of Governors, The Doctors Company

Martha Donovan Hayward

Institute for Healthcare Improvement, Public and Patient Engagement

Marilyn Neder Flack

Executive Director, Association for the Advancement of Medical Instrumentation (AAMI) Foundation
Senior Vice President, Patient Safety Initiatives

Bakul Patel, MSEE, MBA

Associate Director for Digital Health (Acting), Center for Devices and Radiological Health, Food and Drug Administration

Andrew Gettinger, MD

Office of Clinical Quality and Safety, Office of the National Coordinator for Health Information Technology

Amy Helwig, MD, MS

Deputy Director, Center for Quality Improvement and Patient Safety, Agency for Healthcare Research and Quality

Ben Bartolome (Alt: Yahya Shaikh, MD, MPH)

Special Counsel, Office of General Counsel, Federal Communications Commission

Minet Javellana

Center for Clinical Standards & Quality, Centers for Medicare & Medicaid Services

Contributing Staff

Douglas Johnston, RTI Project Director

Stephanie Rizk, RTI Roadmap/Task Force Task Lead

Colene Byrne, RTI Task Force Facilitator

Barry Blumenfeld, RTI Task Force Facilitator

Linda Dimitropoulos, RTI Senior Advisor

[This page intentionally left blank.]

References

- ¹ ONC has developed several general overviews of the value of EHRs, for example, see:
Office of the National Coordinator for Health Information Technology. Benefits of EHRs - Improved Diagnostics & Patient Outcomes. <http://www.healthit.gov/providers-professionals/improved-diagnostics-patient-outcomes>. 2014.
Office of the National Coordinator for Health Information Technology. Benefits of EHRs - Improved Care Coordination. <http://www.healthit.gov/providers-professionals/improved-care-coordination>. 2014.
Office of the National Coordinator for Health Information Technology. Benefits of EHRs - Medical Practice Efficiencies & Cost Savings. <http://www.healthit.gov/providers-professionals/medical-practice-efficiencies-cost-savings>. 2014.
- ² Office of the National Coordinator for Health Information Technology. Report to Congress. Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic Use and Exchange of Health Information. Washington, DC; U.S. Department of Health and Human Services. http://www.healthit.gov/sites/default/files/rtc_adoption_and_exchange9302014.pdf. October 2014.
- ³ Singh H, Thomas EJ, Mani S, Sittig D, Arora H, Espadas D, Khan MM, Petersen LA. Timely follow-up of abnormal diagnostic imaging test results in an outpatient setting: are electronic medical records achieving their potential?. *Arch Intern Med*. 2009; 169(17):1578-86.
- ⁴ Singh H, Wilson L, Petersen LA, Sawhney MK, Reis B, Espadas D, Sittig DF. Improving follow-up of abnormal cancer screens using electronic health records: trust but verify test result communication. *BMC Med Inform Decis Mak*. 2009; 9:49.
- ⁵ Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US Food and Drug Administration databases. *Appl Clin Inform*. 2011; 2: 63-74.
- ⁶ According to the Institute of Medicine, the Learning Health System is a system "in which science, informatics, incentives, and culture are aligned for continuous improvement and innovation, with best practices seamlessly embedded in the delivery process and new knowledge captured as an integral by-product of the delivery experience...". For more on the Learning Health System, see:
<http://iom.edu/~media/Files/Activity%20Files/Quality/VSRT/Core%20Documents/LearningHealthSystem.pdf>
- ⁷ Institute of Medicine. *To err is human: Building a safer health system*. Washington, DC. National Academy Press. 1999.
- ⁸ IOM. *Crossing the Quality Chasm: A new health system for the 21st century*. Washington, DC. National Academy Press. 2001.
- ⁹ Sittig DF, Singh H. A New Socio-technical Model for Studying Health Information Technology in Complex Adaptive Healthcare Systems. *Quality & Safety in Healthcare*. 2010;19 Suppl 3:i68-74.
- ¹⁰ Office of the National Coordinator for Health Information Technology. SAFER Guides – High Priority Practices. <http://www.healthit.gov/safer/guide/sg001>. 2014. Office of the National Coordinator for Health Information Technology. SAFER Guides – Organizational Responsibilities. <http://www.healthit.gov/safer/guide/sg002>. 2014.
- ¹¹ Institute of Medicine. *HIT and Patient Safety: Building Safer Systems for Better Care*. <http://www.iom.edu/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx>. 2011.

- ¹² Office of the National Coordinator for Health Information Technology. Health Information Technology Patient Safety Action & Surveillance Plan. <http://www.healthit.gov/policy-researchers-implementers/health-it-and-safety>. 2013.
- ¹³ Office of the National Coordinator for Health Information Technology. ONC Health IT Safety Program – Progress on Health IT Patient Safety Action and Surveillance Plan. http://www.healthit.gov/sites/default/files/ONC_HIT_SafetyProgramReport_9-9-14_.pdf. 2014.
- ¹⁴ The IOM *Health IT and Patient Safety: Building Safer Systems for Better Care* report further recommended that the Secretary of HHS should recommend to Congress the creation of an independent Federal entity to investigate health IT related safety issues. While this recommendation is seen as an important potential activity, such an entity has not been authorized by Congress, therefore this roadmap for the creation of a national Health IT Safety Center does **not** attempt to serve as such an entity.
- ¹⁵ Food and Drug Administration, Office of the National Coordinator for Health Information Technology, Federal Communications Commission. Food and Drug Administration Safety and Innovation Act (FDASIA): Health IT Report on Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology. <http://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm390588.htm>. 2014.
- ¹⁶ Office of the National Coordinator for Health Information Technology. Federal Health IT Strategic Plan 2015-2020. <http://www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf>. 2015.
- ¹⁷ Food and Drug Administration, Office of the National Coordinator for Health Information Technology, Federal Communications Commission. Food and Drug Administration Safety and Innovation Act (FDASIA): Health IT Report on Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology. <http://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm390588.htm>. 2014.
- ¹⁸ Hydari MZ, Telang R, and Marella WM. Saving Patient Ryan — Can Advanced Electronic Medical Records Make Patient Care Safer? <http://ssrn.com/abstract=2503702>. September 30, 2014.
- ¹⁹ Banger A, Graber M. Recent Evidence the Health IT Improves Safety. Health IT Safety Issue Brief #1. http://www.healthitsafety.org/uploads/4/3/6/4/43647387/brief__1_final_feb11.pdf. Raleigh-Durham, NC: RTI International. 2015.
- ²⁰ Buntin M, Burke M, Hoaglin M, Blumenthal D. The benefits of health information technology: A review of the recent literature. *Health Affairs*. 2011;30(3):464-71.
- ²¹ Jones S, Rudin R, Perry T, Shekelle P. Health information technology: An updated systematic review with a focus on meaningful use. *Ann Int Med*. 2014;160:48-54.
- ²² ECRI Institute. PSO Deep Dive: Health Information Technology. Plymouth Meeting, PA. ECRI Institute. 2012.
- ²³ Mardon R, Olinger L, et al. Health Information Technology Adverse Event Reporting: Analysis of Two Databases. Rockville, MD: Westat; 2014. Available at: http://healthit.gov/sites/default/files/Health_IT_PSO_Analysis_Final_Report_11-25-14.pdf
- ²⁴ Meeks DW, Smith MW, Taylor L, et al. An analysis of electronic health record-related patient safety concerns. *J Am Med Inform Assoc*. 2014;0:1–7. 1
- ²⁵ Schiff GD, Amato MG, Eguale T, et al. Computerised physician order entry-related medication errors: analysis of reported errors and vulnerability testing of current systems. *BMJ Qual Saf*. 2015;0:1–8.

-
- ²⁶ Sparnon E, Marella WM. The Role of the Electronic Health Record in Patient Safety Events. *PA Patient Saf Avis* 2012 Dec;9(4):113-21.
- ²⁷ Friedberg MW, Chen PG, Van Busum KR, et al. Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy. Santa Monica, CA. RAND Corporation. 2013.
- ²⁸ American Medical Association. Improving Care: Priorities to Improve Electronic Health Record Usability. Chicago, IL; American Medical Association. 2014.
- ²⁹ Castro G. Investigations of Health IT-related Deaths, Serious Injuries, or Unsafe Conditions. *ONC Health IT Safety Webinar Series*.
http://www.healthitsafety.org/uploads/4/3/6/4/43647387/webinar_1_full_deck_2014-12-18_v5.pptx. 2014.
- ³⁰ Public Law (PL) 109-41 – The Patient Safety and Quality Improvement Act of 2005 (PSQIA). <http://www.pso.ahrq.gov/legislation/act>. July 29, 2005.
- ³¹ Some task force members would have supported broader functions that were not considered because they are outside of the scope of the Center based on limitations of the potential funding agencies.
- ³² ONC and AHRQ have the ability to collect data related to specific programs and activities separate from any potential Health IT Safety Center. ONC can collect data, for example, related to certification. AHRQ has specific authorities with regard to data collection, including through the Network of Patient Safety Databases.
- ³³ Classen DC, Lloyd RC, Provost L, Griffin FA, Resar R. Development and evaluation of the Institute for Healthcare Improvement Global Trigger Tool. *Journal of Patient Safety*. 2008 Sep;4(3):169-177.
- ³⁴ The Leapfrog Group. CPOE evaluation tool. <https://leapfroghospitalsurvey.org/cpoe-evaluation-tool/>. 2015.
- ³⁵ Classen D, Resar R, Griffin F, et al. 'Global Trigger Tool' Shows That Adverse Events In Hospitals May Be Ten Times Greater Than Previously Measured. *Health Aff*. April 2011; 30(4):581-589.
- ³⁶ Adler L, Yi D; Li M, et al. Impact of Inpatient Harms on Hospital Finances and Patient Clinical Outcomes. *J Patient Saf*. 2015;00: 00 – 00.
- ³⁷ After selecting the executive director and convening the initial advisory board, the host organization and funding agency would, with input from the executive director and advisory board, develop a charter specifying processes and criteria for identification of any subsequent Center executive director and advisory board members.
- ³⁸ Initial sources of evidence should include, but not necessarily be limited to:
- PSO voluntary reported data (AHRQ Common Formats, Health IT Hazard Manager)
 - Medical liability claims data (CRICO, Doctors Company)
 - Sentinel event reports (TJC)
 - eRx/CPOE order data (e.g. ADE Triggers)
 - Provider claims data
 - Post-marketing surveillance data (FDA MAUDE)
 - AHRQ's Network of Patient Safety Databases (NPSD)
 - ONC's Certified Health IT Product List (CHPL)
 - Department of Veterans Health Affairs data
 - State-based hospital safety reporting systems
 - EHR simulation data
 - Analyses of health IT safety events from the peer-reviewed literature

- ³⁹ Bureau of Labor Statistics. Occupational Employment Statistics – May 2014 national Occupational Employment and Wage Estimates, United States.
http://www.bls.gov/oes/current/oes_nat.htm#11-0000. 2014.