Safe Practice Recommendations for Developing, Implementing, and Integrating a Health IT Safety Program
Safe Practice Recommendations for Developing, Implementing, and Integrating a Health IT Safety Program

March 2018
Acknowledgments

We would like to thank our workgroup chair, Partnership Expert Advisory Panel member, Patricia P. Sengstack, DNP, RN-BC, FAAN, of Vanderbilt University, and the entire workgroup for their contributions. The workgroup members identified issues, discussed practices, pondered strategies, and assembled the recommendations and tools for implementation included here. We also wish to thank those who presented and shared valuable information with the workgroup, which helped develop this publication. The multistakeholder workgroup participants and contributors are listed here:

Patricia Sengstack, DPN, RN-BC, FAAN, Workgroup Chair, Vanderbilt University
Don Asmonga, Officer, Health Information Technology, The Pew Charitable Trusts
Geoff Caplea, MD, MBA, Medical Director – Regulatory, Quality, & Patient Safety, Allscripts
Gerry Castro, PhD, MPH, Project Director, Patient Safety Initiatives, Joint Commission on Accreditation of Healthcare
Allen Chen, MD, PhD, MHS, Associate Professor Oncology, Associate Professor Pediatrics, Armstrong Institute for Patient Safety and Quality, The Johns Hopkins Hospital
Andrea Cobb, Texas Medical Association
Brian Crawford, Epic
Mike Favreau, Allscripts
Trisha Flanagan, MSN, RN, CPPS, Director of Patient Safety, athenahealth
Roy Gill, MD, Physician Director of Clinical Content, NextGen Healthcare
Richard Homaday, Senior Solutions Manager – Public Health and Certification, Allscripts
T. Jamison, PIAA
Joe Lewelling, VP, Emerging Technologies and Health IT, Association for the Advancement of Medical Instrumentation (AAMI)
Trish Lugtu, CPHIMS, Constellation, Inc.
Laura Majewski, Manager Clinical Informatics, Beaumont Health System
Wendi Melgoza, Sutter Health System
Mike Midgley, RN, JD, MPH, CPHRM, DFASHRM, President, American Society for Healthcare Risk Management (ASHRM)

P. Divya Parikh, Vice President of Research & Risk Management, PIAA
Jim Russell, Epic
Donna Summers, CNIO, Henry Ford Health System
Tim Swope, Senior Policy Analyst, Bipartisan Policy Center
Feliciano “Pele” Yu, Jr., MD, MSH, MSPH, FHIMSS, Chief Medical Information Officer, Arkansas Children’s Hospital

ECRI INSTITUTE
Ronni Solomon, JD, Executive Vice President and General Counsel
Julia L. Bamdt, MA, Associate Editor
Eloise DeHaan, BS, ELS, Medical Copyeditor
Ellen Deutsch, MD, MS, FAAP, FACS, CPPS, Medical Director
Robert Giannini, NHA, CHTS-IM/CP, Patient Safety Analyst and Consultant
Patricia Giuffrida, MSN, RN, CPHIMS, Patient Safety, Risk and Quality, Health IT Safety
Amy Goldberg-Alberts, MBA, FASHRM, CPHRM, Executive Director, Partnership Solutions
David T. Jamison, Executive Director, Health Devices Group
Scott R. Lucas, PhD, PE, Director, Accident and Forensic Investigation
Jeremy J. Michel, MD, MHS, Health Technology Assessment, ECRI Institute–Penn Medicine AHRQ Evidence-based Practice Center (EPC)
Ben Pauldine, Senior Graphic Designer

Lorraine Possanza, DPM, JD, MBE, FACFOAM, FAPWCA, Program Director, Partnership for Health IT Patient Safety
Anisha Skaniya, MPH, RRT
Amy Tsou, MD, MS, Associate Medical Director, Health Technology Assessment, ECRI Institute–Penn Medicine AHRQ Evidence-based Practice Center (EPC), and Corporal Michael J. Crescenz Department of Veterans Affairs (VA) Medical Center

GORDON AND BETTY MOORE FOUNDATION
We offer special thanks to the Gordon and Betty Moore Foundation for its generous support in building a sustainable private sector infrastructure for effective health information technology (IT) patient safety practices.
Acknowledgments (continued)

EXPERT ADVISORY PANEL

David W. Bates, MD, MSc, Brigham and Women’s Hospital
Kathleen Blake, MD, MPH, American Medical Association
Pascale Carayon, PhD, University of Wisconsin-Madison College of Engineering
Tejal Gandhi, MD, MPH, CPPS, NPSF Lucian Leape Institute, Institute for Healthcare Improvement/National Patient Safety Foundation

Chris Lehmann, MD, Vanderbilt University Medical Center
Peter J. Pronovost, MD, PhD, The Johns Hopkins University School of Medicine
Jeanie Scott, MS, CPHIMS, Veterans Health Administration Office of Informatics and Analytics/Health Informatics
Patricia P. Sengstack, DNP, RN-BC, FAAN, Vanderbilt University

Hardeep Singh, MD, MPH, Michael E. DeBakey VA Medical Center and Baylor College of Medicine
Dean Sittig, PhD, The University of Texas Health Science Center at Houston, School of Biomedical Informatics
Paul Tang, MD, MS, IBM Watson Health

Partnership Collaborating Organizations
EXECUTIVE SUMMARY

Health information technology (IT) is integral to healthcare today. Technologies are being developed for and used daily in all healthcare settings. The health IT ecosystem includes combinations of “home grown” legacy systems, various commercial systems, and a multitude of technology-driven devices (e.g., smart pumps, scales, glucometers, and anesthesia equipment). Use of these technologies can both positively and negatively affect patient safety.

Organizations providing healthcare play a vital role in health IT safety. These technologies are used by a larger and larger group of stakeholders, including the following: medical personnel (physicians, nurses, other staff), IT experts (IT department, help desk staff, systems experts, informatics leaders), safety leaders (patient safety officers, management, quality and risk leaders), and patients. Vendors and developers, people who implement and support technology, and regulators also play roles in technology safety. Each of these stakeholders can play a significant role in identifying new ways to incorporate technology to provide safer care.

Throughout a technology’s life cycle, the following matters arise and can affect patient safety: IT issues (upgrades, coding changes, added or deleted devices, downtimes), governance (regulatory requirements, information governance), and user issues (competency, changes in workflow and communication, variation in appearance of clinical content such as numeric values).

Combined with a fast-paced and continually stimulated environment, these concerns leave little time for stakeholders to proactively assess safety. It is only by working collaboratively that it is possible to benefit from efforts to incorporate health IT safety into an organization’s safety program.

Safe Practice Recommendations

The Partnership for Health IT Patient Safety, a multistakeholder collaborative convened and operated by ECRI Institute, examined the need for integrating health IT safety into an
organization’s safety program, recognizing both the unintended consequences of technology’s use and the potential to improve safety by incorporating technology. The Partnership undertook this task to create a framework for recognizing often-unappreciated technology-related safety issues. Health IT safety is not selectively defined. In part, this is because health IT safety issues are not always clearly identifiable. Health IT safety in some ways is like an iceberg (Figure 1), with the bulk of the potential safety risks, as well as the new potential safety uses, remaining hidden. Clarity and recognition will come only with additional investigation and knowledge.

The Partnership’s work strives to identify and mitigate what exists below the surface. In doing so, Partnership workgroup members developed three safe practice recommendations, which are the building blocks for integrating, collaborating, and embedding (ICE) clinical safety efforts.

Below are the Partnership’s safe practice recommendations for developing, implementing, and integrating a health IT safety program. The Partnership’s work discusses the recommendations and provides tools to facilitate the domains of health IT safety: safe health IT, safe use of health IT, and use of health IT for safety (Sittig and Singh “Electronic”; “Sociotechnical”).

**Figure 1. Health IT Safety = ICE**

**Integrate**

Identify ways to integrate health IT safety into existing programs.

**Collaborate**

Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety.

**Embed**

Embed safety into the culture and daily workflow to achieve a unified vision of health IT safety.
## Table of Contents

Executive Summary vii  
Introduction 3  
Workgroup Process 4  
Recommendations 5  
Discussion 9  
Conclusion 13  
References 14  
Definitions 18  
Tools 20  
INTEGRATE: Preparing To Integrate Health IT Safety –Tools for the Initial Steps  
Infographic: Is Your Patient Safety Event Health IT–Related? 23  
Case Examples—Health IT Safety 24  
Analysis and Reporting Tools Using Standard Format/Standard Taxonomies  
AHRQ Common Formats for Health IT 27  
Health IT Hazard Event Reporting Form 31  
Use Your Own Vendor Reporting Tools 34  
Algorithm and Steps—Review Process for Health IT-Related Issues 35  
Did You Know—Did You Ask?  
Leadership Tool for an Organization 37  
Tool for Providers 38  
User Tool for a Vendor/Developer Organization 39
SAFER Guides 40

COLLABORATE: Working Together To Incorporate Health IT Safety

Health IT Issues Log—Conducting Risk Analysis and Documenting Findings 41

Education and Learning Opportunities

  Leadership/Organizations 42

  Health IT User Education 55

Self-Assessment Questionnaires for a Safety Culture

  Safety Culture Leadership 71

  Safety Culture Health IT Users 76

EMBED: Entrenching Health IT Safety Efforts

  Leadership and Organizations Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan 83

  Health IT Users Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan 84

  Health IT Dashboard 85

  Health IT Safety Program Evaluation Tool 86

Communication and Transparency Tools for a Health IT Safety Program 88

  Sample Safety Memo 89

  Sample Safety Report Feedback Log 90

Appendix 92
Introduction

Anticipating and mitigating the unintended consequences of developing and using health information technology (IT) throughout its life cycle is the focus of a health IT safety program for healthcare facilities, providers, and vendor/developers. Technology risks may not be immediately recognized because the effects of coding changes, upgrades to a particular module, and bugs may not be immediately seen. By incorporating health IT safety into an organization’s general safety program, safety hazards can be identified early on, interventions can be made, and risks can be mitigated.

Health IT safety is analogous to an iceberg. Only the tip is currently visible. Below the surface are the unseen and the unknown—the size and potential impact are yet unclear. Clarity will come only with additional planning, awareness, investigation, and knowledge. Although health IT safety issues may not have triggered events or were unrecognized as the source of risk, they must be taken into consideration when developing a comprehensive risk and safety program. For example, we have come to recognize risks associated with drop-down lists, inadequate information transfer, downtimes, and coding changes, but these may well be only the tip of the iceberg that represents health IT safety concerns.

To facilitate development and integration of a health IT safety program, the Partnership and its multistakeholder workgroup evaluated processes and practices for incorporating health IT safety into a general safety program. “Evidence continues to indicate that health IT safety is dependent not just on EHR [electronic health record] systems themselves, but on a complex interplay of factors, including an institution’s leadership, culture readiness, installation practices, training, and handling of upgrades. Improving safety requires attention to all of these areas.” (ONC “Gettinger”)

With this in mind, the workgroup focused on what was necessary for integrating, collaborating, and embedding health IT safety in an organization. The goal is to prevent the silo-effect of addressing health IT issues in isolation. Using enterprise risk management techniques and considering a sociotechnical model, the workgroup evaluated the components of a health IT safety culture, including the following:

- Committing to health IT safety
- Understanding a just safety culture
- Adequately identifying the involved stakeholders
- Evaluating and using general risk principles
- Employing initial and continuous learning opportunities
- Reporting (including reporting to vendors and by vendors)
- Understanding technology’s function within the sociotechnical environment
- Providing feedback on interventions to strengthen safety efforts and strengthen organizational learning

The general flow and relationship of these components are shown in Figure 2.

Awareness resulting from incorporating these elements helps us to begin to understand what is unknown
or unrecognized—the bulk of the iceberg. The safe practice recommendations for developing, implementing, and integrating a health IT safety program are a timely reminder that health IT safety is an integral part of patient safety. Such safety is best evaluated by looking at the domains of safe health IT, safe use of health IT, and the use of health IT for safety as they exist throughout the technology’s life cycle.

To facilitate the execution and integration of a health IT safety program, the Partnership developed this tool kit including the following:

- Algorithms for early recognition and analysis of health IT issues
- Case examples
- Learning modules
- Reporting tools
- Self-assessments

The toolkit additionally offers references and outside resources to help clarify and supplement the materials provided. The toolkit applies to all stakeholders regardless of where they are in their program’s development and execution. By increasing health IT safety awareness, looking at the safety culture, and assessing safety in the daily work structure, organizations can work to improve the domains of health IT safety—safe health IT, safe use, and development of new ways of executing technology for safety.

**WORKGROUP PROCESS**

The Partnership’s safety workgroup, chaired by Partnership Expert Advisory Panel member Patricia Sengstack, DPN, RN-BC, FAAN, Vanderbilt University, included a multistakeholder membership with subject matter experts, researchers, IT professionals, healthcare providers and provider organizations, vendor/developers, and professional organizations.

**Meetings.** The workgroup met monthly from February 2017 through July 2017. Anonymous and identified workgroup participation was enabled using collaboration software. Monthly meetings provided a method to gather information from risk and safety professionals, to identify the parts of a successful safety program in provider and vendor settings, and to assimilate this information for developing safe practice recommendations.

**Literature search.** Before the workgroup began meeting, a medical librarian conducted a literature search of empiric and gray literature from 2009 through 2016. A key word search using PubMed, Medline, EMBASE, CINAHL, and Scopus identified the recent literature regarding health IT safety plans and programs. The identified materials were screened and reviewed by ECRI Institute’s patient safety analysts. Selected materials from this search appear in the attached references. These materials and other relevant information was presented to the workgroup in order to develop these safe practice recommendations.

**Event identification and analysis.** Events submitted for the time period July 2014 through November 2016 were analyzed. Learnings from this analysis and from the literature facilitated tool development. Selected de-identified events are provided in the tool, “Case Examples,” to facilitate recognition of health IT–related issues. These examples can be used as the basis of use cases, which may be helpful in examining a technology’s functioning throughout its life cycle.

In evaluating health IT’s role in safety events, analysts used the algorithm appearing in Figure 3. This algorithm was modified from a process that is used to evaluate medication errors. Event analysis points to the importance of continued reporting, including reporting to and by vendors. Often data initially indicates little direct evidence that events are related to technology, and only through event analysis can possible relationships to the technology be discovered. Importantly, it is also during this time that technology’s
use for error prevention can be detected.

Development of safe practice recommendations. Once all of the information was collated—including information from the literature review, event analysis, and expert examples of effective health IT safety programs—the workgroup discussed and compiled three safe practice recommendations. These safe practices are to be used in developing, implementing, and integrating an organization’s health IT safety program.

RECOMMENDATIONS

The Partnership’s safe practice recommendations aim to integrate health IT safety, encourage collaboration, and embed (ICE) a health IT safety culture into the organizations’ safety program. Before identifying ways to integrate health IT safety into existing safety programs, organizations must first look at the life cycle of technology from the initial choice of technology through implementation, use, upgrades, and phase out. Proactively identifying and exchanging information about health IT–related risks, hazards, and events, as is done in traditional risk programs, is elemental to integrating health IT into a safety program (Table 1). A basic step is to provide training and continuous learning about the safe use of technology and its potential to both mitigate and cause risk. Measurement is needed to evaluate the effectiveness of the risk strategies that are used. Matching performance metrics (something vendors frequently track) to clinically relevant measures sheds light on effective safety efforts. For example, metrics on downtime, uptime, alert overrides, system response times, open orders, number of clicks, and time spent on tasks can provide valuable insight into potential improvements and risk avoidance. However, these efforts are effective only when all stakeholders are working together on such safety efforts.

Next, collaboration is needed not only to convene the necessary stakeholders, but to actively engage them in safety efforts. The stakeholders are a broad group, including patients, providers, vendor/developers, organizational leadership, technology specialists, regulators, legislators, informaticists, human factor researchers, risk and safety specialists, payers, and those in cyber security. Each of these stakeholders has a role and impacts health IT safety. It is important that stakeholders own their roles in addressing and mitigating health IT safety issues. Moreover, it is important that these stakeholders work together to identify opportunities to use the technology for safety. To incorporate health IT effectively, those working with the technology must be incorporated into teams with existing safety program members. The composition of these teams may vary, based on the organization’s size or area of specialization (vendor, provider).

Finally, safety must be embedded into the culture and daily workflow in an organization. A lesson taken from safety efforts in other industries emphasizes the importance of “anchoring changes” in the organization’s culture (NCHRP). This ensures that safety will persist as an ongoing goal as it becomes part of the organization’s culture. Transforming and embedding a safety culture is accomplished by sharing the value of safety, changing behaviors to achieve these safety goals, and employing safety strategies as part of the cultural model (NCHRP).

By implementing these three safe practice recommendations, organizations can develop, implement, and integrate health IT safety into their organizations’ risk and safety programs. The strategies, rationale, and tools to facilitate incorporation of each of the recommendations are provided in this toolkit. As the unknown aspects of the health IT iceberg come to the surface, those working with the technology can integrate, collaborate, and embed new safety elements into their culture and daily workflow to achieve a unified vision of safe health IT and safe use and additional uses of technology for safety (see Figure 1).
TABLE 1. SAFE PRACTICE RECOMMENDATIONS FOR DEVELOPING, IMPLEMENTING, AND INTEGRATING A HEALTH IT SAFETY PROGRAM

Below are examples of various types of policies to facilitate the use of health IT in patient identification.*

<table>
<thead>
<tr>
<th>Safe Practice Recommendation</th>
<th>Strategies to Implement</th>
<th>Stakeholder</th>
<th>Tools and References (see Safe Practice Recommendations [p. 22] for rationale and stakeholders)</th>
</tr>
</thead>
</table>
| **Integrate:** Identify ways to integrate health information technology (IT) safety into existing safety programs | Using General Safety Program* principles for health IT safety  
* Risk Identification  
• Use both proactive (e.g., failure modes, safety assessments, awareness studies) and reactive strategies (e.g., investigations, root-cause analyses [RCAs], common cause analysis) for advancing safety and safety issues  
• Integrate identifying and reporting health IT–related risk into risk assessments and activities  
* Risk Analysis/Assessment  
• Assess for safety before introducing new technology and/or upgrades (e.g., test scripts, use-case testing, information flow evaluations, simulation)  
• Encourage reporting (e.g., patient safety organization [PSO], IT, vendor)  
• Ensure active participation by health IT subject matter experts (SMEs) in organizational safety meetings, investigations, analysis, resolutions, and uses of technology for safety  
* Risk Mitigation  
• Incorporate health IT safety into enterprise risk strategies  
• Encourage reporting (PSOs, IT, vendor, other)  
• Implement vendor recommendations to avoid internal workarounds  
• Create a health IT–related reporting system with a common reporting language  
• Use walkarounds, huddles, and summaries to report issues for action  
* Risk Control  
• Test and monitor implementations, upgrades, and modifications, as appropriate across the life cycle  
• Report health IT–related patient safety events to the vendor or developer  
• Identify safety standards for implementation  
• Evaluate reporting, tracking, and transparency in issue resolution  
* Risk Assumption  
• Develop a health IT–related event analysis process  
• Develop metrics for health IT processes and outcomes | • Leadership  
• Providers  
• Vendors  
• Provider organizations | • Risk Identification  
 o Risk Assessment Tools (AHRQ)  
 o Safety Briefings Tool (IHI)  
 o Quick Safety Issue 34: Daily Safety Briefings (Joint Commission)  
 o Infographic: Is Your Patient Safety Event Health IT–Related? (p. 23)  
 o Case Examples (p. 24)  
 o SAFER Guides (ONC) (p. 40)  
• Risk Analysis/Assessment  
 o Health Information Technology Through the Lens of Patient Safety (IHI/NPSF “Health” [course description])  
 o Take 5: Safe Use of Health Information Technology (Joint Commission [audio file])  
 o SAFER Guides (ONC) (p. 40)  
• Risk Mitigation  
 o Algorithm—Health IT Issue Analysis (p. 35)  
 o Reporting Tools  
 o AHRQ Common Formats (p.27)  
 o Health IT Hazard Manager—Pennsylvania (AHRQ)  
 o SAFER Guides (ONC) (p. 40)  
• Risk Control  
 o Health IT Issues Log (p. 41)  
 o SAFER Guides (ONC) (p. 40)  
• Risk Assumption  
 o The Digital Transformation: How Technology is Helping (and Hurting) Health Care (IHI)  
 o SAFER Guides (ONC) (p. 40) |
### TABLE 1. SAFE PRACTICE RECOMMENDATIONS FOR DEVELOPING, IMPLEMENTING, AND INTEGRATING A HEALTH IT SAFETY PROGRAM

<table>
<thead>
<tr>
<th>Safe Practice Recommendation</th>
<th>Strategies to Implement</th>
<th>Stakeholder</th>
<th>Tools and References (see Safe Practice Recommendations [p. 22] for rationale and stakeholders)</th>
</tr>
</thead>
</table>
| Collaborate: Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety | Continuous Learning  
- Provide training and periodic updates for competency-based learning and sharing of information about health IT-related safety issues  
- Strengthen relationships (e.g., provider-vendor) so that issues are appropriately escalated and resolved  
- Identify and work to resolve safety issues (involve appropriate parties, consult vendor, participate in multistakeholder analysis and development activities)  
- Conduct health IT simulations  
- Include patient and family participation, as appropriate, encouraging their input into safety systems and checks  
- Provide learning and sharing of health IT-related issues, hazards, and successes  
| Checklists/Check-ups  
- Gather information and raise awareness via regularly scheduled activities (e.g., leadership walkarounds)  
- Incorporate health IT safety (e.g., initiatives, events, guidance) into work assessments  
- Use portals and information exchanges  
- Provide training and periodic updates for competency-based learning and sharing of information about health IT-related safety issues  
- Become involved in safety initiatives | Vendors  
- Providers  
- Patients  
- Provider organization  
- Leadership | Educational PowerPoint slides  
- Leadership and Vendor/Developer Organizations (p. 42)  
- Health IT User (p. 55)  
- Self-Assessment Checklists/Check-ups  
- Did You Know—Did You Ask? (p. 37)  
- Leadership and Organization Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan (p. 83)  
- Health IT Users Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan (p. 84)  
- Risk Control  
- Health IT Issues Log (p. 41) |
<table>
<thead>
<tr>
<th>Safe Practice Recommendation</th>
<th>Strategies to Implement</th>
<th>Stakeholder</th>
<th>Tools and References (see Safe Practice Recommendations [p. 22] for rationale and stakeholders)</th>
</tr>
</thead>
</table>
| Embed: embed safety into the culture and daily workflow to achieve a unified vision of health IT safety | • Continually evaluate safety  
  o Identify current safety awareness through self-assessments  
  o Create a nonpunitive culture that encourages reporting and open discussion of safety issues (PSO reporting, Safe Tables, vendor dialogue, and user groups)  
  o Periodically assess the organization’s safety culture (self-assessment questionnaires, other surveys)  
  o Implement survey-specific improvement strategies, and monitor results  
  • Daily safety  
  o Encourage increased transparency (dashboards, follow-up information, and safety updates to staff)  
  o Share survey results and conduct periodic updates to monitor status  
  o Implement safety huddles/briefings  
  • Developing a just culture for safety  
  o Create a nonpunitive culture that encourages reporting and open discussion of safety issues (PSO reporting, Safe Tables, vendor dialogue, and user groups)  
  o Identify transparent safety systems with accountability, consequences, and acknowledgements  
  o Integrate safety into the culture rather than counting on one particular leader or individual alone  
  o Assess health IT as part of the patient safety culture | • Leadership  
  • Providers  
  • Vendors | Check-up for Continuously Evaluating Safety  
  • Health IT Dashboard (Safety Program Evaluation Tool) (p. 85)  
  • Patient Safety Leadership WalkRounds™ (IHI)  
  • Feedback and Communication Tools for a Health IT Safety Program  
  o Sample Safety Memo (p. 89)  
  o Sample Safety Report Feedback Log (p. 90)  
  Daily Safety  
  • AHRQ TeamSTEPPS—Safety Huddles  
  • Safety Briefings Tool (IHI)  
  • Conducting a Morning Briefing (AHRQ)  
  Developing a Just Culture for Safety  
  • Develop a Culture of Safety (IHI)  
  • Patient Safety Leadership WalkRounds™ (IHI) |
DISCUSSION

In 2015, the National Patient Safety Foundation (now IHI/NPSF) identified eight recommendations for achieving total systems safety including “ensuring that technology is safe and optimized to improve patient safety” (IHI/NPSF “New”). Singh and Sittig in 2016 additionally pointed out that it is important to “make health IT-related patient safety an organizational priority by securing commitment from organizational leadership [. . . and to] develop an environment that is conducive to detecting, fixing and learning from system vulnerabilities” (Singh and Sittig). Finally, the Bipartisan Policy Center’s Health Innovation Initiative in 2017 presented key principles for a health IT framework for safety, as follows (BPC):

- Health IT safety should be integrated into broader patient safety efforts
- Patient safety efforts should address the entire health IT life cycle
- Patient safety is a shared responsibility
- A nonpunitive, learning system approach will drive improvement
- Health IT safety approaches should be evidence-based and data-driven

These recommendations and principles apply generally to all stakeholders using and developing health IT. The Partnership’s safe practice recommendation approach increases awareness and optimization of health IT safety and looks for meaningful safety strategies that stakeholders can use to round out and incorporate health IT safety into a general safety program.

These total system safety recommendations influence technology’s incorporation throughout healthcare and not in a single provider, provider organization, or developer. Useful in fulfilling total system safety is Singh and Sittig’s Health Information Technology Safety Measurement (HITS) Framework as seen in Figure 4. This framework incorporates the important health IT safety domains—safe IT, safe use of health IT, and using health IT to improve safety—and applies them to the sociotechnical environment. While this emphasizes that the domains should be incorporated into all aspects of the health IT safety program, it also delineates the role of measurement. Improvements in patient outcomes and overall safety are the goals.

The Partnership’s workgroup in identifying the framework for developing, implementing, and integrating health IT safety into a risk and safety program considered Figure 4’s schema. But to comprehensively evaluate the impact of health IT safety, it was essential to first consider the sociotechnical system and pair it with the elements of an enterprise risk model to ensure that health IT would not remain confined to organizational siloes.

Let’s first look at the sociotechnical framework, which includes the following:

- Hardware and software
- Clinical content
- Human-computer interface
- People
- Workflow and communication
- Internal organizational features
- External rules and regulations
- Measurement and monitoring

See Figure 5.

NPSF’s eight recommendations for total system’s safety are as follows:

1. Ensure that leaders establish and sustain a safety culture
2. Create centralized and coordinated oversight of patient safety
3. Create a common set of safety metrics that reflect meaningful outcomes
4. Increase funding for research in patient safety and implementation science
5. Address safety across the entire care continuum
6. Support the health care workforce
7. Partner with patients and families for the safest care
8. Ensure that technology is safe and optimized to improve patient safety

Figure 4. Health Information Technology Safety Measurement (HiTS) Framework

<table>
<thead>
<tr>
<th>Sociotechnical Work System*†</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Health IT Safety Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe HIT</td>
</tr>
<tr>
<td>Integrity</td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td>Confidentiality</td>
</tr>
<tr>
<td>Safe use of HIT</td>
</tr>
<tr>
<td>Usability</td>
</tr>
<tr>
<td>Complete use</td>
</tr>
<tr>
<td>Correct use</td>
</tr>
<tr>
<td>Using HIT to improve safety</td>
</tr>
<tr>
<td>Surveillances &amp; Optimisation</td>
</tr>
</tbody>
</table>

Italicized text denotes domain principles

Changes in standards, regulations, policy and practice

Expected Measurement Impact

- Integration of HIT safety with existing clinical risk management & patient safety program
- Organisational learning
- Shared responsibility
- 360° assessment
- Refinement of measurement tool/strategies

Feedback to EHR developers and healthcare organisations

* Includes eight technological and non-technological dimensions.
† Includes external factors affecting measurement such as payment systems, legal factors, national quality measurement initiatives, accreditation and other policy and regulatory requirements.
EHR, electronic health record.

Figure 5. Pairing the Sociotechnical and Enterprise Risk Models

- Technology
- Strategic
- System measurement and monitoring
- Clinical content
- Human-computer interface
- People
- Hazard
- Operational
- Financial
- Human capital
- External rules, regulations, and pressures
- Organisational policies, procedures, and culture
- Workflow and communication
- Legal/regulatory
The sociotechnical model aligns nicely with the elements of an enterprise risk strategy, whose elements are as follows:

- Technology
- Clinical and patient safety consideration
- Hazards
- Human capital concerns
- Financial considerations
- Operational processes
- Legal and regulatory issues
- Strategic elements

Combining all of these elements ensures that the necessary health IT considerations are incorporated when attempting to assess, measure, prioritize, and mitigate risk. The synergies were further clarified in presentations to the workgroup by both healthcare providers and vendor/developers. The elements of their existing programs align with the core of both the sociotechnical model and enterprise risk strategies. However, many of the programs reviewed were freestanding and not part of the organization’s overall risk and safety programs. This emphasizes that these models must be considered together to have a continuous process for safety. This is seen in Figure 6 when overlaying the safe practice recommendations on these models. Note that the process can begin at any of the three safe practice recommendation areas because different organizations may be further along in their processes. It is then possible to move forward or backward as necessary to achieve safety throughout the technology’s life cycle (for further clarification see Figure 6).

The Partnership’s three ICE recommendations, including strategies and tools for implementation by stakeholders, are outlined in detail in Table 1. We will discuss the specific aspects of each of the safe practice recommendations and the coordinating tools below.

**Integrate.** To prepare to integrate health IT safety into a safety program, simplify the recognition of health IT events by performing appropriate training and provide opportunities for ongoing learning. These continued opportunities for learning are essential as technologies are added, upgraded, replaced, and interconnected. It is important that stakeholders recognize ongoing safety concerns and can identify whether errors might be related to the technology, so that solutions can be crafted.

For example, in 2017, Carayon and co-authors noted that duplicate medication errors increased after a new EHR implementation. The authors identified contributing factors including the EHR’s design and task-related changes that occurred (e.g., multiple persons entering orders for the same patient at the same time). The authors also pointed to

Figure 6. Building on a Core to Inform Health IT Safety
“organization-related changes in handoff communication with duplicate orders placed before and after change of shift.” To comprehensively analyze these issues, Carayon et al. highlighted the need for a sociotechnical systems approach to assess and address safety. A structured approach helps guarantee that the technology is considered in the setting of use. To assess the implementation of the new technology, look back at the overlaid model in Figure 6 or use other risk tools, such as a root-cause analysis, to analyze the increased number of duplicated orders. Additionally, a proactive assessment may consider such tools as failure mode and effects analysis.

Using a comprehensive systems approach and not confining the evaluation of health IT safety to silos facilitates a proactive approach to assessing safety. It is essential to consider the domains of health IT. This begins with technology development, choice, and implementation and then evaluates use, upgrades, and integration with other systems throughout the technology’s life. To complete safety assessments, it is important to perform pre- and post-implementation testing, as well as upgrade testing. Included in any assessments should be screening of events for potential health IT involvement (e.g., red flags, metrics); investigating contributing factors (e.g., burnout); and using reports and reporting tools (e.g., structured reporting, help desk, vendor reporting) and techniques (e.g., safety huddles, walkarounds) to increase awareness, facilitate classification, and enable review of safety concerns (See Table 1 for tools and strategies).

Other tools for identifying health IT-related issues include the following:

- Looking at core measures for adverse events related to health IT use
- Matching performance metrics to clinically relevant measures
- Looking at issues such as alert firing patterns (Wright et al.)
- Evaluating rule logic, especially after configuration changes
- Conducting monitoring and testing strategies (looking at systems—e.g., clinical decision support [CDS] and others, upgrades, vendor issues, and change logs, including rule and logic changes)
- Conducting failure mode and effects analyses (FMEAs), being mindful that FMEA may not capture the interrelationship between systems (Borycki and Keay)

The development of use cases provides yet another way to evaluate health IT safety using safety principles. Use cases shed light on the ability of a user to “execute a particular task in a timely manner without error.” (Middleton et al.) Executing the safe practices to integrate health IT safety is possible only when all of the key stakeholders are included and working collaboratively.

Collaborate. Collaboration involves convening the necessary stakeholders, including users, vendor/developers, organizations, patients, and others, to proactively address health IT safety and the safety domains. Ongoing and shared learning is part of collaborating on safety. Learnings from the analysis of reported events, hazards, near misses along with strategies used to address workarounds provides valuable insight if shared. Education includes not only initial instruction, but also ongoing learning, shared practices, and continued assessment of competencies. Note that the ONC Workforce Development Programs webpage provides suggested role-based competencies (for more information see https://www.healthit.gov/providers-professionals/health-it-competencies-and-learning-resources).

Using tools to increase transparency and to facilitate analysis will not only strengthen relationships, but will also provide opportunities for shared analysis and safety improvements. With increased transparency through collaboration, prioritization and resolution of issues becomes more agile. It will be important to fully utilize the provisions of the 21st Century Cures Act (Public Law 114-255) to broaden the scope of awareness of health IT safety issues. Only then will this shared safety culture provide for effective safety practices and shared learnings. This will drive innovation. Tools to implement this safe practice and facilitate learning are included in this toolkit (see Table 1).

Embed. As mentioned above, it is important to embed safety into the culture and daily workflow. Leadership on all levels must support and encourage individuals developing, using, and affected
by health IT to speak up so safety issues can be brought to light. Further, leaders need to encourage staff reporting. This will make health IT issues more readily recognizable and avoidable. This is the foundation of a safety culture.

A “safety culture within an organization is exemplified by the shared values and behaviors that demonstrate a commitment to safety over competing goals” (NCHRP). A safety culture accommodates and encourages reporting and shares and communicates learning. These tenets of a safety culture additionally support the first two safe practice recommendations.

For an effective safety culture, it is important that a safety climate is created. This safety climate must be informed, flexible, and just (i.e., blame-free). A just culture is created in many ways and can have many component parts. Sittig and Singh proffer that safety huddles not only increase awareness of EHR-related safety, but that the “blame-free” culture created by safety huddles supports open communication, and that using this proactive approach could allow earlier identification of safety issues and swift resolution as issues emerge.” (Menon et al.)

Provided in this toolkit are assessments for an overview of an organization’s safety climate. This is the first step in determining whether teams, departments, and individuals prioritize and embed safety as part of the organization’s culture.

The safe practice recommendations taken together with the suggested tools and strategies provide a way to develop, implement, and integrate, health IT safety into a risk and safety program (see Table 1 and the “Tools” section of this report). The tools incorporated here will facilitate approaches for identifying, managing, and advancing health IT safety within provider and vendor/developer organizations. It is through these shared learnings that additional safety innovations will be able to exceed current expectations.

CONCLUSION

Technology today is an integral part of healthcare. Embedding health IT safety into existing risk and safety programs throughout the organization will help to ensure that health IT is safe, that it is used safely, and that it is used for safety. (Singh and Sittig). Widespread use and associated reliance on health IT makes it even more important to understand both the risks and the benefits of technology. “EHRs won’t improve unless we study them, collect data on what went wrong, and—importantly—resolve to use those data to make EHR systems better.” (Payne) To facilitate this, the Partnership for Health IT Patient Safety has examined ways to develop, implement, and integrate an effective health IT safety program in both healthcare and vendor/developer organizations. Three safe practice recommendations and the tools needed to facilitate the incorporation of health IT into a safety framework are provided here. It is time that all stakeholders—those providing and receiving care and those developing and implementing products—improve and facilitate the provision of care by working together to drive and incorporate health IT safety. By identifying and prioritizing safety issues, technology will be developed and used safely throughout its life cycle, but more importantly, new safety uses for health IT will result.
REFERENCES


Agency for Healthcare Research and Quality (AHRQ). Department of Health and Human Services:


Institute for Healthcare Improvement (IHI):


Institute for Healthcare Improvement/National Patient Safety Foundation (IHI/NPSF).

Health information technology through the lens of patient safety. http://www.npsf.org/?page=healthit


The Joint Commission:


Quick safety issue 34: daily safety briefings - a hallmark of high reliability. 2017 Jun 19 [cited 2017 Jul 27] https://www.jointcommission.org/issues/article.aspx?Article=p0A7zc0O0nDmT7bt%2f0U10eyf7dG2A%2f8V3Xy%2bynmdVCE%3d

Sentinel event alert 54: safe use of health information technology. https://www.jointcommission.org/sea_issue_54/


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


Sittig DF, Singh H:


Definitions

A common understanding of terminology is needed to discuss safety practices. The workgroup includes the following definitions to provide a common language for stakeholders.

culture—“Shared perceptions about what is good, right, important, valued, rewarded, supported and expected. Culture is shaped by policies, practices and procedures, the values of personalities of people in the organization, and leadership.” (IHI)

EHR—Electronic health record.

EHR-related system flaw—Any characteristic of an EHR or of its interactions with other healthcare systems that has the potential to worsen care quality or patient outcomes. Flaws may be introduced during the specification, design, configuration, or continuous-improvement phases of the EHR life cycle. (Middleton et al.)

e-iatrogenesis—Patient harm caused at least in part by the application of health information technology. (Sittig; Weiner et al.)

enterprise risk management (ERM)—In healthcare, ERM promotes a comprehensive framework for making risk management decisions that maximize value protection and creation by managing risk and uncertainty and their connections to total value. ERM includes the following domains: operational, clinical/patient safety, strategic, financial, human capital, legal/regulatory, technology, and hazard. (ASHRM’s; Midgley)

event—A discrete, auditable, and clearly defined occurrence. (NQF)

hazard, health IT—A characteristic of any health IT application or its interactions with any other system that increases the risk that care processes will be compromised and patients harmed. (AHRQ “Walker”)

hazardous (or “unsafe”) condition—A circumstance (other than a patient’s own disease process or condition) that increases the probability of an adverse event. (Joint Commission “PS”)

health IT—A broad concept that encompasses an array of technologies used to store, share, and analyze health information. (ONC “Basics”) “Health information technology (health IT) devices comprise the hardware and software that are used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention of disease. . . . Although health IT is often considered to be synonymous with electronic health records (EHRs) and EHR components such as computerized provider order entry (CPOE) or clinical decision support, health IT also includes administrative or practice management systems, automated dispensing systems, laboratory information systems, and diagnostic imaging systems. (Joint Commission “Castro”)

incident—A patient safety event that reached the patient whether or not the patient was harmed. (NQF)
just culture—A culture that recognizes that individual practitioners should not be held accountable for system failings over which they have no control. A just culture also recognizes that many individual or “active” errors represent predictable interactions between human operators and systems in which they work. However, in contrast to a culture that touts “no blame” as its governing principle, a just culture does not tolerate blameworthy behavior, such as a conscious disregard of clear risks to patients or gross misconduct (e.g., falsifying a record, performing professional duties while intoxicated). (ACHE and NPSF)

patient safety—Preventing and mitigating harm caused by errors of omission or commission that are associated with healthcare and involving the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur. (NQF)

patient safety event—An event, incident, or condition that could have resulted or did result in harm to a patient. (Joint Commission “PS”)

risk management—The identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks. An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events. (BusinessDictionary)

safety culture—“The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of an organization’s health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perception of the importance of safety, and by confidence in the efficacy of preventative measures. (IHI/NPSF “Leading”; Study Group)

sociotechnical approach—“The sociotechnical approach regards individual systematic components as a single, complex adaptive system in which the technology changes the way some people organize and conduct their work and the way some people change the technology. . . . One key aspect of the sociotechnical approach is that one cannot analyze any of these inter-related dimensions in isolation, rather one must always recognize their dependence and interaction with each other.” (Sittig and Singh “Sociotechnical”)

technology-related error—An error related to a technology that would not have happened but for the use of this technology. (Carayon et al.)

total systems safety—Safety that is systematic and uniformly applied (across the total process). (Joint Commission “Pronovost”)

unintended consequences—The effects of technological interventions that deviate from the functionality expected from the original system design. (Koppel and Chen)
Tools

Included in the following section are tools that facilitate developing, implementing, and integrating a health IT safety program. As you review your processes, you may discover that one or more parts of each of the three steps have been completed. Use these tools and references to evaluate current practices and to augment what is currently in place.

Integrate. The first part of integrating a health IT safety program includes leadership commitment, stakeholder identification, and recognition of health IT-related issues and hazards. Provided here are tools, including an infographic, deidentified case examples, reporting tools and techniques, a process algorithm, and links to resources, which will facilitate these steps. A first step may be to evaluate the information found in the SAFER Guides. (Sittig and Singh “More Proactive”)

Standard reporting tools are referenced here. It is also important to emphasize that reports should also be made to vendors.

Collaborate. Working together collaboratively involves communicating issues with health IT and identifying new ways to use the technology for safety. Included here are an issues log that allows for prioritization of issues, self-assessment questionnaires, and education and learning tools. Collaboration also involves openly sharing information. Such information can be effectively communicated to those who are positioned to take action by collaborating through walkarounds, daily huddles, and routine assessments.

Embed. Finally, embedding health IT safety into the organizations culture is essential for success and sustainability. Included here are two scorecards and action plans, which relate to the self-assessment surveys; a health IT dashboard; and a communication and transparency tool, with templates for a memo and for feedback. Although reporting is essential, communicating what has been done keeps stakeholders informed and emphasizes a commitment to safety. This not only shows that safety is a priority, but it further strengthens the safety culture.

The list of attached tools that follows can be found as part of this toolkit and at the Health IT website.
INTEGRATE: Preparing To Integrate Health IT Safety—Tools for the Initial Steps

Infographic: Is Your Patient Safety Event Health IT–Related?
Case Examples—Health IT Safety
Analysis and Reporting Tools Using Standard Format/Standard Taxonomies
  AHRQ Common Formats for Health IT
  Health IT Hazard Event Reporting Form
  Use Your Own Vendor Reporting Tools
Algorithm and Steps—Review Process for Health IT-Related Issues
Did You Know—Did You Ask
  Leadership Tool for an Organization
  Tool for Providers
  User Tool for a Vendor/Developer Organization
SAFER Guides

COLLABORATE: Working Together To Incorporate Health IT Safety

Health IT Issues Log—Conducting Risk Analysis and Documenting Findings
Education and Learning Opportunities
  Leadership/Organization Education
  Health IT User Education
Self-Assessment Questionnaires for a Safety Culture
  Safety Culture Leadership
  Safety Culture Health IT Users

EMBED: Entrenching Health IT Safety Efforts

Leadership and Organizations Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan
Health IT Users Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan
Health IT Dashboard
Health IT Safety Program Evaluation Tool
Communication and Transparency Tools for a Health IT Safety Program
  Sample Safety Memo
  Sample Safety Report Feedback Log
Safe Practice Recommendations for Developing, Implementing, and Integrating a Health IT Safety Program

Health IT Safety = ICE

Integrate
Identify ways to integrate health information technology (IT) safety into existing safety programs.

Rationale for practice: Integrating health IT into a safety program presumes that the entity has a robust safety program in place. The elements of a good risk program include risk identification, risk prevention, risk mitigation, risk control, and risk assumption. Those identified risks are analyzed, solutions are developed and implemented, and results are monitored and adjusted as needed. Creating awareness of the health IT issues and concerns and identifying new ways that health IT promotes safety is a primary reason for integrating health IT into a safety program. It is important to secure leadership support by leveraging these existing structures whenever possible and to evaluate issues that can arise across the life cycle of the technology or software.

Stakeholders impacted: Providers, vendor/developers, leadership, healthcare, and supplier organizations

Collaborate
Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety.

Rationale for Practice: A safety program that addresses health IT safety needs to include a broader group of stakeholders than that which is incorporated into a general safety program. This may vary by entity (vendor/developer, provider, healthcare organization). Included in this group are the vendor/developers, information technology experts and staff, and those providers not only using the technology, but expert in how to address risks and the potential benefits of using technology for safety. Such collaboration supports a continuing learning environment.

Stakeholders impacted: Providers, vendor/developers, leadership, patients

Embed
Embed safety into the culture and daily workflow to achieve a unified vision of health IT safety.

Rationale for Practice: Health IT is ubiquitous and facilitates safety, but may also have unintended consequences. When health IT safety is embedded into an organization’s culture, it is possible to prioritize risks and recognize the benefits of health IT in a nonpunitive transparent learning environment.

Stakeholders impacted: Providers, vendor/developers, patients, leadership
Is Your Patient Safety Event Health IT–related?

Definition: A health information technology (IT)–related patient safety event is any event triggered by, or related to, the technology that has caused patient harm, has the potential to cause patient harm, or that causes a delay in treatment or misdiagnosis. These errors would not occur but for the use of technology.

- Display is confusing or not accurate
- The data is difficult to locate
- The data is lost, corrupted, or deleted
- The data is difficult to enter
- The workflow does not match our workflow

- Computerized provider order entry (CPOE) is difficult
- Medication error
- Pharmacy error

- System malfunction
- System unavailable
- Downtime
- Power outage
- Connectivity issue
- Interface issue
- Interoperability issue

- Incorrect

- Excessive demand on the human memory to recall information

- Excessive information
- Excessive nonspecific recommendations or alerts
- Improper recommendations
- Faulty reference information
- Missing recommendations or safeguards
## Case Examples—Health IT Safety

The Case Examples—Health IT Safety tool can be used when conducting education or raising awareness related to issues, concerns, or unintended consequences of the use of health information technology (IT).

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Sociotechnical Dimensions</th>
<th>Reporting</th>
<th>ICE Actions/Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a mammogram is copied, the tags allowing clinicians to distinguish between up, down, left, and right are missing.</td>
<td>Hardware and software Clinical content Workflow and communication</td>
<td>Radiology, Equipment/device function—incorrect image orientation Data quality</td>
<td>INTEGRATE: Assess whether any other modalities are affected. Review contributing/causative factors. COLLABORATE: Involve front-line staff, information technology (IT) staff, and vendor/developer to develop actions required, deploy fixes. EMBED: Monitor and evaluate fixes. Track action plan’s effectiveness, and communicate learnings.</td>
</tr>
<tr>
<td>A pediatric patient’s weight was entered incorrectly in triage, taken and recorded in pounds when the entry should be made in kilograms. The incorrect weight was used to determine medication doses.</td>
<td>Hardware and software People Workflow and communication</td>
<td>Electronic health record (EHR)—clinical documentation Ergonomics—data entry or selection Usability Notify vendor</td>
<td>COLLABORATE: Involve senior leadership, frontline staff, IT staff, purchasing, and vendor to develop mitigation strategies. Develop education and competency tools. EMBED: Evaluate workflow and resources. Communicate learnings.</td>
</tr>
<tr>
<td>When ordering an Epi-Pen, the medication search shows only the pediatric dose and not the adult dose. This could lead to an inappropriate underdose of the ordered medication.</td>
<td>Human/computer interface People Clinical content</td>
<td>EHR—computerized provider order entry (CPOE) Ergonomics—data entry or selection Usability</td>
<td>COLLABORATE: Involve providers, pharmacy, and IT staff to evaluate functionality. Develop functional keyword selection. Educate appropriate staff. EMBED: Monitor and evaluate fixes.</td>
</tr>
<tr>
<td>When a patient’s chart is unmerged because more than one patient’s information is contained in a chart, the process is not communicated to all downstream computer systems.</td>
<td>People Workflow and communication Policy/Procedure/ Environment</td>
<td>Admission, discharge, and transfer (ADT) system Ergonomics—data entry or selection Data quality</td>
<td>INTEGRATE: Assess downstream departments involved. COLLABORATE: Involve senior leadership, appropriate stakeholders (downstream departmental staff) and IT staff. Develop standard operating procedure and policy. Provide education and evaluate. EMBED: Develop procedural communication plan. Evaluate workflow. Communicate learnings.</td>
</tr>
<tr>
<td>Case Study</td>
<td>Sociotechnical Dimensions</td>
<td>AHRQ Common Formats</td>
<td>Health IT Hazard</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>When multiple patient charts are open, alerts and alert responses might not file to the correct patient.</td>
<td>Hardware and software Clinical content Workflow and communication System measurement and monitoring</td>
<td>EHR—clinical decision support (CDS) Ergonomics—alert fatigue</td>
<td>Decision support</td>
</tr>
<tr>
<td>Due to undefined naming conventions used with patient name, laboratory results were filed in the error queue.</td>
<td>Hardware and software Workflow and communication</td>
<td>EHR—clinical documentation Equipment/device function—loss or delay of data</td>
<td>Local implementation</td>
</tr>
<tr>
<td>A system-wide downtime of the EHR occurred that lasted longer than 10 hours, caused by the failure of a critical piece of hardware. Some users were unable to access downtime reports on the computers identified for use during downtime to access historical records.</td>
<td>Hardware and software Clinical content Workflow and communication</td>
<td>Hardware</td>
<td>Hardware failure</td>
</tr>
<tr>
<td>Patient received a medication from an ambulatory pharmacy site that was ordered for another patient with the same name. The wrong patient was selected from the picklist.</td>
<td>Human/computer interface People Workflow and communication</td>
<td>EHR—CPOE Ergonomics—information display</td>
<td>Usability</td>
</tr>
<tr>
<td>A patient with a pending swallow evaluation received an incorrect diet. There is no safeguard in place in the EHR to warn clinicians to change the diet order when a swallow evaluation is ordered.</td>
<td>Clinical content Human/computer interface People Workflow and communication</td>
<td>EHR—CDS Equipment/device function</td>
<td>Decision support</td>
</tr>
<tr>
<td>Case Study</td>
<td>Sociotechnical Dimensions</td>
<td>AHRQ Common Formats</td>
<td>Health IT Hazard</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Propofol was ordered for a patient. Propofol is contraindicated when a</td>
<td>Hardware and software</td>
<td>EHR--CPOE Equipment/device function</td>
<td>Usability</td>
</tr>
<tr>
<td>patient has an egg allergy. An egg allergy is listed in the patient’s</td>
<td>Clinical content Workflow and communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chart. The egg allergy was entered as a free text allergy and was not</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mapped; therefore, no alert fired notifying the staff of the contraindication.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device data from the monitoring system is not flowing into patient EHR.</td>
<td>Clinical content Workflow and communication System measurement and monitoring</td>
<td>EHR--clinical documentation Equipment/device</td>
<td>Local implementation</td>
</tr>
</tbody>
</table>
Analysis and Reporting Tools Using Standard Format/Standard Taxonomies

AHRQ COMMON FORMATS FOR HEALTH IT

Use this form to report any patient safety event or unsafe condition involving a defect, failure, or incorrect use of a device, including an HIT device. A device includes an implant, medical equipment, or medical/surgical supply (including disposable product). An HIT device includes hardware or software that is used to electronically create, maintain, analyze, store, or receive information to aid in the diagnosis, cure, mitigation, treatment, or prevention of disease and that is not an integral part of (1) an implantable device or (2) an item of medical equipment.

For defects or events discovered prior to market approval or clinical deployment, do not use this form. If the event also involves a medication or other substance, please complete the Medication or Other Substance form in addition to this form. Narrative detail can be captured on the Healthcare Event Reporting Form (HERF). Highlighted fields are collected for local facility and Patient Safety Organization (PSO) use. This information will not be forwarded to the Network of Patient Safety Databases (NPSD).

1. Which of the following best describes the event or unsafe condition? CHECK ONE:
   a. Device defect or failure, including HIT
   b. Use error
   c. Combination or interaction of device defect or failure and use error
   d. Unknown

2. What type of device was involved in the event or unsafe condition? CHECK ONE:
   a. Implantable device (i.e., device intended to be inserted into, and remain permanently in, tissue)
   b. Medical equipment (e.g., walker, hearing aid)
   c. Medical/surgical supply, including disposable product (e.g., incontinence supply)
   d. HIT device

3. At the time of the event, was the device placed within the patient’s tissue? CHECK ONE:
   a. Yes
   b. No
   c. Unknown

4. Did the event result in the device being removed? CHECK ONE:
   a. Yes
   b. No
   c. Unknown

5. What is the name (brand or generic) of the device, product, software, or medical/surgical supply?

6. What is the name of the manufacturer?
7. Which of the following identifiers are known? CHECK ALL THAT APPLY:

a. ☐ Model number
b. ☐ Software version
c. ☐ Firmware version
d. ☐ Serial number
e. ☐ Lot or batch number
f. ☐ Other unique product identifier
g. ☐ Date of expiration
h. ☐ Unique Device Identifier
i. ☐ Asset tag
j. ☐ No identifiers known

8. What is the model number?

9. What is the software version?

10. What is the firmware version?

11. What is the serial number?

12. What is the lot or batch number?

13. What is the type of other unique product identifier?

14. What is the other unique product identifier?

15. What is the expiration date?
   ___ / ___ / ___

16. What is the Unique Device Identifier (UDI)?

17. What is the asset tag number?

18. Was a device intended for single use involved in the event or unsafe condition (including use of a reprocessed single-use device)? CHECK ONE:

   a. ☐ Yes
   b. ☐ No
   c. ☐ Unknown

19. Was a device intended for a single use reused in the event or unsafe condition? CHECK ONE:

   a. ☐ Yes
   b. ☐ No
   c. ☐ Unknown
20. Did the event or unsafe condition involve a medication or other substance? 

CHECK ONE:

a. Yes
b. No
c. Unknown

IF THE EVENT OR UNSAFE CONDITION DID NOT INVOLVE AN HIT DEVICE

STOP This form is complete.

IF THE EVENT OR UNSAFE CONDITION INVOLVED AN HIT DEVICE, ANSWER QUESTIONS 21-26

21. Which of the following best characterizes the type of HIT device related to the event or unsafe condition?

CHECK ONE:

a. Administrative/billing or practice management system
b. Automated dispensing system
c. Electronic health record (EHR) or component of EHR
d. Human interface device (e.g., keyboard, mouse, touchscreen, speech recognition system, monitor/display, printer)
e. Laboratory information system (LIS), including microbiology and pathology systems
f. Radiology/diagnostic imaging system, including picture archiving and communications system (PACS)
g. Other: PLEASE SPECIFY

22. Which component of the administrative/billing system?

CHECK ONE:

a. Master patient index
b. Registration/appointment scheduling system
c. Coding/billing system
d. Unknown
e. Other: PLEASE SPECIFY

23. Which type or component of the EHR?

CHECK ONE:

a. Computerized provider order entry (CPOE) system
b. Pharmacy system
c. Electronic medication administration record (e-MAR)
d. Clinical documentation system (e.g., progress notes)
e. Clinical decision support (CDS) system
f. Unknown
g. Other: PLEASE SPECIFY
### Event ID:

**Initial Report Date (HERF Q1):** ________________

#### 24. Which of the following describes the circumstances involving the HIT device in the event or unsafe condition?**

CHECK ALL THAT APPLY:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>□ Incompatibility between devices</td>
</tr>
<tr>
<td>b.</td>
<td>□ Equipment/device function</td>
</tr>
<tr>
<td>c.</td>
<td>□ Equipment/device maintenance</td>
</tr>
<tr>
<td>d.</td>
<td>□ Hardware failure or problem</td>
</tr>
<tr>
<td>e.</td>
<td>□ Network failure or problem</td>
</tr>
<tr>
<td>f.</td>
<td>□ Ergonomics, including human/device interface issue</td>
</tr>
<tr>
<td>g.</td>
<td>□ Security, virus, or other malware issue</td>
</tr>
<tr>
<td>h.</td>
<td>□ Unexpected software design issue</td>
</tr>
<tr>
<td>i.</td>
<td>□ Unknown</td>
</tr>
<tr>
<td>j.</td>
<td>□ Other: PLEASE SPECIFY</td>
</tr>
</tbody>
</table>

#### 25. Which problem(s) resulted from the equipment/device function problem? **CHECK ALL THAT APPLY:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>□ Loss or delay of data</td>
</tr>
<tr>
<td>b.</td>
<td>□ System returns or stores data that does not match patient</td>
</tr>
<tr>
<td>c.</td>
<td>□ Image measurement/corruption issue</td>
</tr>
<tr>
<td>d.</td>
<td>□ Image orientation incorrect</td>
</tr>
<tr>
<td>e.</td>
<td>□ Incorrect test results</td>
</tr>
<tr>
<td>f.</td>
<td>□ Incorrect software programming calculation</td>
</tr>
<tr>
<td>g.</td>
<td>□ Incorrect or inappropriate alert</td>
</tr>
<tr>
<td>h.</td>
<td>□ Other: PLEASE SPECIFY</td>
</tr>
</tbody>
</table>

#### 26. Which ergonomics or human/device interface issue(s)?** CHECK ALL THAT APPLY:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>□ Hardware location (e.g., awkward placement for use)</td>
</tr>
<tr>
<td>b.</td>
<td>□ Data entry or selection (e.g., entry or selection of wrong patient, wrong provider, wrong drug, wrong dose)</td>
</tr>
<tr>
<td>c.</td>
<td>□ Information display or interpretation (e.g., font size, color of font, location of information in display screen)</td>
</tr>
<tr>
<td>d.</td>
<td>□ Alert fatigue/alarm fatigue</td>
</tr>
<tr>
<td>e.</td>
<td>□ Other: PLEASE SPECIFY</td>
</tr>
</tbody>
</table>

---

**Thank you for completing these questions.**

---

**OMB No. 0935-0143**  
Exp. Date 10/31/2014  
Public reporting burden for the collection of information is estimated to average 10 minutes per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: AHRQ Reports Clearance Officer, Attention: PRA, Paperwork Reduction Project (0935-0143), AHRQ, 540 Gaither Road, Room #5306, Rockville, MD 20850.  

AHRQ Common Formats - Hospital Version 1.2 - April 2012  
Device or Medical/Surgical Supply, including Health Information Technology (HIT)  
Page 4 of 4
HEALTH IT HAZARD EVENT REPORTING FORM

The Health IT Hazard Event Reporting Form is a tool for identifying, categorizing, and resolving health information technology (IT) hazards. The tool allows healthcare organizations and software vendor organizations to learn about potential health IT–related hazards and work to resolve them, including the collection and use of data to communicate potential and actual adverse effects. The Health IT Hazard form allows an organization to look at an event from discovery to causation, the impact of the event, and the hazard control plan. An Excel version of the tool can be accessed at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/HIT_Hazard.xls.

### Health IT Hazard Reporting Form

<table>
<thead>
<tr>
<th>What is being reported:</th>
<th>Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Near miss</td>
</tr>
<tr>
<td></td>
<td>Unsafe condition</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event date:</th>
<th>Event discovery date:</th>
</tr>
</thead>
</table>

**Brief event description:**

### How was the hazard discovered?

- Retrospective analysis
- Local information technology (IT) implementation and testing (DBV)
- Value-added reseller
- End-user report (any clinician)
- Automated error log
- Patient or lay-caregiver report
- Vendor reported (any vendor)
- Chart review
- Other: Please specify

### Stage of discovery

- Software specification
- Vendor programming
- Customer configuration
- Customer programming
- Testing
- Training
- Initial go-live
- Production use
- Upgrade

### How long was the hazard present in the system when it was discovered?

- Hours (up to 23):
- Days (up to 30):
- Weeks (up to 51):
- Months

### How was the hazard communicated?

- Unknown
- Communicated internally
- Reported to software vendor
- Published report (including electronic publication)
- Informal communication with vendor user group

### Usability

- Information hard to find
- Difficult data entry
- Excessive demand on human memory
- Suboptimal support of teamwork (situation awareness)
- Confusing information display
- Inadequate feedback to the user
- Mismatch between real workflows and health IT
- Mismatch between user expectations (mental models) and health IT
- Other: Please specify

### Data quality

- IT design contributed to entry of data in the wrong patient’s record
- Organization contributed to entry of data in the wrong patient’s record
- Patient information/results routed to the wrong recipient
- Discrepancy between database and displayed, printed, or exported data
- Unpredictable elements of the patient’s record available only on paper/scanned documents
- Lost data
- Inaccurate natural language processing
- Virus or other malware
- Other: Please specify

### Decision support

- Excessive nonspecific recommendations/alerts
- Faulty recommendation
- Missing recommendation or safeguard
- Inadequate clinical content
- Inappropriate level of automation
- Other: Please specify

### Vendor factors

- Suboptimal interfaces between applications (and devices)
- Nonconfigurable software
- Faulty vendor configuration recommendation
- Unusable software implementation tools
- Inadequate vendor testing
- Inadequate vendor software change control
- Inadequate control of user access
- Faulty software design (specification)
- Other: Please specify
### Local Implementation
- Faulty local configuration or programming
- Inadequate local testing
- Inadequate project management
- Inadequate software change control
- Inadequate control of user access
- Suboptimal interface management
- Other: Please specify

### Other factors
- Inadequate training
- Excessive workload (including cognitive)
- Inadequate organizational change management
- Inadequate management of system downtime or slowdown
- Unclear policies
- Compromised communication among clinicians (i.e., hand-offs)
- Interactions with other (non-health IT) care systems
- Physical environment (e.g., hardware location, lighting, engineering)
- Hardware failure
- Inadequately secured data
- Use error in the absence of other factors
- Other: Please specify

### Has this hazard affected a care process?
- Yes
- No
- Unknown

### What level of risk is there that this hazard could affect a care process if it is not controlled?
- High
- Medium
- Low

### If the hazard were to affect a care process, how likely is it that an end user would notice before a patient was harmed?
- High
- Medium
- Low

### Best estimate of how many patients could be affected if this hazard is not fixed?
- <10
- 10-100
- >100

### What is the most serious/worst harm that could happen if hazard is not fixed?
- Death
- Severe harm
- Moderate harm
- Mild harm
- No harm

### What was the effect of this hazard on patients?
- Did not reach patient
- Reached patient but caused no harm
- Harmed patient
- Unknown

### Best estimate of how many patients were harmed?
- <10
- 10-100
- >100

### What is the estimated duration of the harm to the patient?
- Long term (one year or greater)
- Temporary (less than one year)
- Unknown

### Type of harm
- Physical
- Psychological (to the patient)
- Financial (to the patient)
- Reputational (to the patient)
- Unknown

### How quickly must this hazard be controlled?
- If hazard is in production: control hazard within 1 month
- If hazard is in production: control hazard within 6 months
- If hazard is not yet in production: delay implementation until software is fixed
- If hazard is in production: URGENT—fix software or remove it from use within 24 hours
- Do not control—the risks exceed the benefits. No further hazard control plan information is required.
- Other: Please specify

---

©2018 ECRI INSTITUTE
<table>
<thead>
<tr>
<th>First control step</th>
<th>Second control step</th>
<th>Third control step</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Vendor software fix</td>
<td>☐ Training for end users</td>
<td>☐ Training for end users</td>
</tr>
<tr>
<td>☐ Local IT configuration change</td>
<td>☐ Care-process change</td>
<td>☐ Care-process change</td>
</tr>
<tr>
<td>☐ Local IT custom programming</td>
<td>☐ Policy change</td>
<td>☐ Policy change</td>
</tr>
<tr>
<td>☐ Training for local IT</td>
<td>☐ Other: Please specify</td>
<td>☐ Other: Please specify</td>
</tr>
</tbody>
</table>

**How complete is the control/correction of this hazard?**

- ☐ Complete
- ☐ Partial—additional steps needed

**Second control step**

- ☐ Vendor software fix
- ☐ Local IT configuration change
- ☐ Local IT custom programming
- ☐ Training for local IT

**How complete is the control/correction of this hazard?**

- ☐ Complete
- ☐ Partial—additional steps needed

**Third control step**

- ☐ Vendor software fix
- ☐ Local IT configuration change
- ☐ Local IT custom programming
- ☐ Training for local IT

**How complete is the control/correction of this hazard?**

- ☐ Complete
- ☐ Partial—additional steps needed

**Plan**

**Who needs to approve the hazard control plan?**

- ☐ Clinical leadership
- ☐ Administrative leadership
- ☐ End user representatives
- ☐ Local IT
- ☐ Software vendor
- ☐ Informatics/Human factors

- ☐ Quality/Safety
- ☐ Risk management
- ☐ Medical records
- ☐ Facilities and engineering
- ☐ Legal
- ☐ Other: Please specify

**Who will implement the hazard control plan?**

- ☐ Clinical leadership
- ☐ Administrative leadership
- ☐ End user representatives
- ☐ Local IT
- ☐ Software vendor
- ☐ Informatics/Human factors

- ☐ Quality/Safety
- ☐ Risk management
- ☐ Medical records
- ☐ Facilities and engineering
- ☐ Legal
- ☐ Other: Please specify
USE YOUR OWN VENDOR REPORTING TOOLS

Algorithm and Steps—Review Process for Health IT–Related Issues


<table>
<thead>
<tr>
<th>Steps</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient safety event reported • Determine whether immediate/interim actions are needed</td>
<td>• HIT Hazard Taxonomy Form • AHRQ Common Formats – Device v1.2 Form • IT Help Desk Logs</td>
</tr>
<tr>
<td>IDENTIFY: Determine whether the reported issue is health IT–related • Health IT–related? YES • Health IT–related? NO — Determine whether technology can help to mitigate the issue: • Can technology help? If YES, go to REVIEW • Can technology help? If NO, determine other solution</td>
<td>Use Infographic and Case Examples to determine safe health IT or safe use of health IT</td>
</tr>
<tr>
<td>ASSESS: Investigate health IT contributing factors Consider sociotechnical dimensions: • Hardware and software • Clinical content • Human-computer interface • People • Workflow and communication • Internal organizational policies, procedures, environment, and culture • External rules, regulations, and pressures • System measurement and monitoring</td>
<td>Use Health IT Issues Log to conduct risk assessment and document findings Sociotechnical dimensions Sittig and Singh (“Sociotechnical”): • Safe health IT (to address safety concerns unique to the technology) • Using IT safely (to optimize and facilitate its use) • Using IT for safety (to monitor and improve patient safety)</td>
</tr>
<tr>
<td>REVIEW: Use patient safety, risk or quality/internal IT/vendor to investigate and analyze to determine health IT contributing factors Consider hazard manager contributing factors: • Usability • Data quality • Decision support • Vendor factors • Local implementation • Other factors</td>
<td>Consider AHRQ Common Formats Contributing Factors: • Incompatibility between devices • Equipment/device function • Equipment/device maintenance • Hardware failure or problem • Network failure or problem • Ergonomics, including human/device interface issues • Security, virus, or other malware issues • Unexpected software design issues • Other • Risk stratification tools • Proactive risk assessments • Failure mode and effects analysis</td>
</tr>
<tr>
<td>COLLABORATE: Collaborate with subject matter experts (SMEs) to determine risk score, conduct gap analysis, and assign priority to identify solutions and long-term adjustments</td>
<td></td>
</tr>
<tr>
<td>DEVELOP: Determine actions required, assign accountability, and conduct testing to ensure readiness for implementation</td>
<td></td>
</tr>
<tr>
<td>DEPLOY: Implement appropriate fixes; provide updates to users</td>
<td></td>
</tr>
<tr>
<td>REMEDIATE: Monitor and evaluate fixes to identify any other systems that may be impacted, as well as validity of fix moving forward</td>
<td>Use Health IT Dashboard to track, monitor, and communicate need for additional remediation</td>
</tr>
<tr>
<td>TRACK: Determine the plan’s effectiveness • Is action plan effective? YES • Is action plan effective? If NO, return to DEVELOP</td>
<td></td>
</tr>
<tr>
<td>COMMUNICATE: Report learnings, strategies for addressing findings, and status to all stakeholders • Vendor • Provider organizations • Users</td>
<td></td>
</tr>
</tbody>
</table>

©2018 ECRI INSTITUTE 35
Algorithm Review Process for Health IT-Related Issues

Patient Safety Event

Immediate/Interim action for patient safety

IDENTIFY Health IT-related?

Yes

ASSESS Health IT contributing factors

No

Other sources for the error have been identified

Can technology help?

No

Other solutions

Yes

REVIEW & COLLABORATE Conduct investigation

Safety analyst Internal IT Vendor

DEVELOP

No

DEPLOY

Yes

REMEDIATE

User Provider organization Vendor

TRACK Action plan effective?

COMMUNICATE
Did You Know—Did You Ask?

LEADERSHIP TOOL FOR AN ORGANIZATION

WHY IS IT IMPORTANT TO ESTABLISH A HEALTH IT SAFETY PROGRAM?

Leadership should recognize that health information technology (IT)–related safety concerns, issues, events, near misses, or hazards can result in patient harm. Integrating a health IT safety program into an existing safety program using an enterprise risk management (ERM) approach will mitigate risk by preventing patient harm using a proactive approach. Healthcare leaders must commit to safety and then actively engage in a health IT safety program. Establishing, leading, and embedding a culture of safety are essential components of preventing or reducing errors and improving overall health care quality and outcomes.

DID YOU KNOW?

☐ Health IT safety is not easily defined because it depends not just on electronic health record (EHR) systems but also on a number of complex sociotechnical factors, including leadership, culture, planning, training, installation, upgrades, and other sociotechnical factors. (AHIMA)
☐ Leadership support is essential if health IT safety is to be an organization-wide priority.
☐ Although risks may not always be apparent, they can have significant implications for patient safety. (Menon)
☐ The successful integration of health IT safety program will require collaboration between leadership, users, and vendors.

DID YOU ASK?

☐ Do we incorporate health IT safety into our existing safety programs?
☐ Do we educate our leaders and staff on safe health IT, the safe use of health IT, and using health IT to improve safety?
☐ Do we exhibit leadership support for health IT safety?
☐ Do we encourage a nonpunitive environment for reporting health IT safety concerns, issues, events, bugs, errors, near misses, and hazards?
☐ Do we provide transparent communication and feedback on reported potential or actual health IT–related safety concerns, events, issues, bugs, errors, near misses, and hazards?
TOOL FOR PROVIDERS

WHAT IS A HEALTH IT SAFETY PROGRAM AND WHY IS IT ESSENTIAL?

Health information technology (IT) is part of the daily workflow, and health IT safety should be embedded into daily activities. This can be done by ensuring that a health IT safety program is part of any existing patient safety program. This program should include all technologies that are used for patient care and care coordination. Health IT safety must be proactive. It must consider and address the life cycle of the technology as well as the sociotechnical elements that make up the complex healthcare environment.

It is imperative that a health IT safety program embeds a nonpunitive culture, obtains leadership support, establishes a proactive approach to safety, works collaboratively with vendors and developers on solutions, and identifies optimizations. Such a program also provides continuous learning. Identifying creative ways to collaborate and report potential safety issues (e.g., huddles, walkarounds, briefings) will positively affect safety.

DID YOU KNOW?

☐ Unreported or underreported health IT–related safety events can lead to patient harm.

☐ Safe health IT, the safe use of health IT, and using health IT safely is the responsibility of all health IT stakeholders.

☐ A health IT safety program encourages reporting and open discussion of safety concern, issues, events, bugs, errors, near misses, or hazards in a nonpunitive environment to all avenues, including vendors.

DID YOU ASK?

☐ Do I know how to recognize whether health IT might have contributed to a safety event?

☐ Do I know how to report a health IT–related safety event and whether it should be reported to my vendor or developer?

☐ Do I know what is done after I report a health IT–related concern, issue, event, bug, error, near miss, or hazard?
USER TOOL FOR A VENDOR/DEVELOPER ORGANIZATION

WHAT IS THE VENDOR/DEVELOPER ROLE IN A HEALTH IT SAFETY PROGRAM?

The EHR Developer Code of Conduct (2016) emphasizes that vendors and developers have a responsibility and an obligation to work with all stakeholders to improve care, increase efficiencies, enhance patient safety, and provide better outcomes. Proactively addressing health information technology (IT) safety can be accomplished, in part, by encouraging reporting of health IT safety concerns, issues, events, bugs, errors, near misses, or hazards throughout software’s life cycle.

Vendors and developers should be committed to safety and take steps to educate staff on health IT safety issues; work in collaboration with clients to develop safe, usable systems; and provide transparent communication regarding all health IT–related safety issues to improve patient outcomes and mitigate risk.

DID YOU KNOW?

☐ Patient safety is a shared responsibility among all stakeholders including vendors and developers, provider organizations, and users.

☐ Bugs, interoperability, and/or usability issues in the software can lead to potential or actual safety issues, events, near misses, or hazards, which can result in patient harm.

DID YOU ASK?

☐ Do we readily communicate health IT–related safety concerns, issues, events, bugs, errors, near misses, or hazards to clients?

☐ Are we receptive to safety concerns, issues, events, bugs, errors, near misses, or hazards reported by our clients, and do we act on them in a timely manner?

☐ Do we provide users with opportunities to participate in the design and testing of our software?

☐ Do I know how to report a safety concern?
SAFER Guides

SAFER Guides were created by the Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services. The nine guides look at EHR safety from foundational, infrastructure, and clinical process perspectives and recommend practices for the safety and safe use of EHRs.

System Configuration (https://www.healthit.gov/safer/sites/safer/files/guides/safer_system_configuration.pdf)
System Interfaces (https://www.healthit.gov/safer/sites/safer/files/guides/safer_system_interfaces.pdf)
Test Results Reporting and Follow-Up (https://www.healthit.gov/sites/default/files/safer_test_results_reporting.pdf)
Clinician Communication (https://www.healthit.gov/safer/sites/safer/files/guides/safer_clinician_communication.pdf)
Health IT Issues Log—Conducting Risk Analysis and Documenting Findings

The Health IT Issues Log is used to gather information about electronic health record (EHR)-related issues, hazards, concerns, and unintended consequences. The log helps document and track health IT issues, hazards, and events. Additionally, it provides a means to capture how the issue was identified, assessed, and reviewed. It helps identify what is needed to develop, deploy, and remediate the issue, hazard, or concern. Keeping this information in a central place allows users to track and communicate the action plan and to monitor successes or the need for additional activities. An Excel version of the tool can be accessed at Health IT Issues Log.
Leadership/Organization Education: Developing, Implementing, and Integrating a Health IT Safety Program

Learning Objectives

- Understand the impact of health information technology (IT) safety on the organization
- Recognize the importance of incorporating health IT into your safety program
- Use the ICE model to identify strategies and solutions
- Show what leaders can do to build a health IT safety culture
What is a Health IT–Related Safety Event?

A health IT–related patient safety event is any event triggered by, or related to, the technology that has caused patient harm, has the potential to cause patient harm, or that causes a delay in treatment or misdiagnosis. These errors would not occur but for the use of technology.

Carayon et al. (2017)

Why Should Leaders Care?

Health IT related safety events, near misses, or hazards can cause:

- Damage to internal and external reputation
- Negative patient outcomes, including decreased patient satisfaction
- Compromised workplace safety
- Diminished workforce/user satisfaction
- Disrupts workflow
The Importance of Developing, Implementing, and Integrating a Health IT Safety Program

- Prioritizing safety
  - Increase awareness of health IT safety
    - Identify events and near misses
    - Identify needed solutions
  - Decrease the incidence of health IT–related safety incidents/risks/hazards
  - Ensure proactive versus reactive (early detection, near misses)
  - Optimize processes (workflow)
  - Make continuous vendor improvements
  - Reinforce the existing safety culture
  - Increase reporting of health IT safety issues, events, hazards, and near misses
  - Realize cost savings

Framework for Integrating a Health IT Safety Program

Leadership and staff commitment to health IT safety → Define a culture of safety → Incorporate organizational patient safety strategy and commit resources → Apply improvement methods, considering human factors and reliability science
Developing, Implementing, and Integrating a Health IT Safety Program

- Health IT safety should not be separated in organizational silos.
- Instead, health IT safety—
  - Requires a systems approach
  - Involves leadership support
  - Is best integrated into the existing patient safety program
  - Is viewed as an integral part of the healthcare sociotechnical system
  - Requires a cross-functional, multidisciplinary teams to develop solutions

Spartan Policy Center (2017)

A Health IT Safety Program That Looks Below the Surface Requires:

- ICE model
  - Integrate
  - Collaborate
  - Embed
Developing, Implementing, and Integrating a Health IT Safety Program

Integrate

Identify ways to integrate health information technology (IT) safety into existing safety programs

Multiple Stakeholders

Health IT Safety Program—Strategies to Integrate Health IT Safety

- Leverage existing structures and integrate health IT safety into established risk and safety programs.
- Develop a comprehensive safety plan.
  - Identify current safety program and program elements
  - Test and monitor implementation, upgrades, and modifications, as appropriate across the life cycle
  - Integrate identifying and reporting health IT–related risks into risk activity assessments and activities
  - Encourage and facilitate reporting (patient safety organizations [PSOs], IT vendor, others)
Health IT Safety Program—Strategies to Integrate Health IT Safety

- Involve the stakeholders
  - Identify the stakeholders who will need to be included in a safety structure
  - Integrate leadership and necessary personnel into safety programs
  - Integrate subject matter experts (SMEs), IT, chief medical information officer (CMIO), chief nursing informatics officer (CNIIO), human factors engineers, and others who are not already included in safety activities into safety and risk programs
  - Engage IT staff support in safety-issue triage, analysis, monitoring, reporting, and resolution
  - Include patients and families, as appropriate, encouraging their input into safety systems and checks

Developing, Implementing, and Integrating a Health IT Safety Program

Health IT Safety Process—ICE

Integrate
Identify ways to integrate health information technology (IT) safety into existing safety programs

Collaborate
Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety

Multiple Stakeholders
Health IT Safety Program—Strategies to Collaborate

- A safety culture should incorporate technology as an essential component for preventing or reducing health IT-related errors.
  - Broaden the safety program by integrating health IT safety into the overall safety culture
  - Identify transparent safety systems with accountability, consequences, and acknowledgements
  - Ensure that health IT safety efforts address the entire health IT life cycle
  - Promote each relationship (e.g., client, vendor, providers, provider organizations, IT, public, private, patient) as a collaborative partnership

Developing, Implementing, and Integrating a Health IT Safety Program

Health IT Safety Process—ICE

Integrate
Identify ways to integrate health information technology (IT) safety into existing safety programs

Collaborate
Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety

Embed
Embed safety into the culture and daily workflow to achieve a unified vision of health IT safety

Multiple Stakeholders
Health IT Safety Program—Strategies to Embed Safety into Culture and Workflow

- Recognize that while health IT facilitates safety, it can also negatively affect safety. It is important that all stakeholders work collaboratively to embed safety and safety solutions.
  - Provide opportunities for continuous learning and share health IT-related issues, hazards, and successes
  - Assess health IT as part of the patient safety culture
  - Maximize workflows to embed safety
  - Identify safety standards for implementation
  - Encourage reporting, tracking, and transparency in issue resolution
  - Integrate safety into the culture rather than in a single particular leader or individual

Case Study Radiology Issue—Using the ICE Model

- When a mammogram is copied, the tags allowing clinicians to distinguish between up, down, left, and right were missing
  - INTEGRATE: Assess whether any other modalities are affected and review contributing/causative factors
  - COLLABORATE: Involve front-line staff, IT staff, and vendor(s) to develop actions and deploy fixes
  - EMBED: Monitor and evaluate fixes, track whether action plan is effective, modify if needed, and communicate learnings
Case Study Software Updates—Using the ICE Model

- An update to the electronic health record (EHR) software resulted in patient headers cutting key information from the display
  - **COLLABORATE**: Involve IT staff and vendor(s) to develop action plans and test and deploy appropriate fixes
  - **EMBED**: Monitor and evaluate fixes, track whether action plan is effective, modify if needed, and communicate learnings

Improve Health IT Safety by Sharing Information About These Suggested Event Types

- Unexpected EHR-related downtime lasting more than eight hours
- Interruptive alerts that have fired more than 100 times with a 100% override rate
- Erroneous displays of laboratory test results or medications
- Roll-back to an older version of EHR software (e.g., a software upgrade affected the system’s function)
- Instances in which a data backup failed to reload properly
- Data losses affecting more than 100 patients
- Software calculation errors affecting more than 100 patients
- System configuration errors affecting more than 100 patients

*Sittig et al, (2014)*
What Can Leadership Do?

- Support the health IT safety effort
- Increase awareness
- Provide adequate resources
- Encourage a “Just Culture”
- Make health IT safety transparent

Tools to Aid Implementation

- SAFER Guides (ONC)
- Sentinel Event Alert 54: Safe use of health information technology (Joint Commission)
- Risk assessment tools (AHRQ)
- Algorithm–Health IT Issue Analysis
- Reporting tools
- Health IT issues log
- Patient Safety Leadership WalkRounds™ (IHI)
- Safety briefings tool (IHI)
- Quick Safety Issue 34: daily safety briefings (Joint Commission)
- AHRQ TeamSTEPPS–Safety Huddles
- Conducting a morning briefing (AHRQ)
Tools to Aid Implementation (Cont’d)

- Health information technology through the lens of patient safety (IHI/NPSF)
- Take 5: safe use of health information technology (Joint Commission [audio file])
- The digital transformation: how technology is helping (and hurting) health care (IHI)
- Infographic: Health IT Awareness, case examples
- AHRQ common formats
- Health information technology hazard manager (Pennsylvania; AHRQ)
- Health IT issue log/dashboard
- Educational PowerPoint
- Checklists

References

Thanking the Workgroup Members for Developing, Implementing, and Integrating a Health IT Safety Program

Chair: Patty Sengstack, DPN, RN-BC, Vanderbilt University

- Don Asmonga, The Pew Charitable Trust
- Geoff Caplea, Allscripts
- Gerard Castro, The Joint Commission
- Allen Chen, Johns Hopkins Medicine
- Andrea Cobb, Texas Medical Association
- Brian Crawford, Epic
- Mike Faysou, Allscripts
- Trisha Flanagan, athenahealth
- Roy Gill, NextEon Healthcare
- Richard Hornaday, Allscripts
- T. Jamison, PIAA
- Joe Lewelling, AAMI
- Trish Lugli, Constellation, Inc.
- Laura Majewski, Beaumont Health System
- Wendell Malgoz, Sutter Health System
- Mike Midgley, RN, JD, MPH, ASHRM
- P. Divya Parikh, PIAA
- Jim Russell, Epic
- Donna Summers, Henry Ford Health System
- Tim Swope, Bipartisan Policy Center
- Pèle Yu, Jr., Arkansas Children’s Hospital

ECRI Institute:
- Roni Solomon, JD, Executive Vice President and General Counsel
- Ellen Deutsch, MD, MB, FAAP, FACS, CPPS, Medical Director
- Robert Giannini, NHA, CHTS-IM/CP, Patient Safety Analyst and Consultant
- Patricia Giuffrida, MSN, RN, CPHIMs, Patient Safety and Health IT Safety
- Amy Goldberg-Alberts, MBA, FASHRM, CPHRM, Executive Director, Partnership Solutions Patient Safety, Risk, and Quality
- Scott R. Lucas, PhD, PE, Director, Accident and Forensic Investigation
- Jeremy J. Michel, MD, MHS, Health Technology Assessment, ECRI-Penn Medicine AHRQ Evidence Based Practice Center (EPC)
- Lorraine Possanza, DPM, JD, MBE, FACFOAM, FAPWCA, Senior Patient Safety, Risk, and Quality Analyst
- Arisha Skaria, MPH, FRT
- Amy Tsou, MD, MSc, Senior Research Analyst, Health Technology Assessment, ECRI–Penn Medicine AHRQ Evidence Based Practice Center (EPC)

Partnership Expert Advisory Panel

- David W. Bates, MD, MSc, Brigham and Women’s Hospital
- Kathleen Blake, MD, MPH, American Medical Association
- Pascale Carayon, PhD, University of Wisconsin-Madison College of Engineering
- Tejal Gandhi, MD, MPH, National Patient Safety Foundation
- Chris Lehmann, MD, Vanderbilt University Medical Center
- Peter J. Pronovost, MD, PhD, The Johns Hopkins University School of Medicine
- Jeanie Scott, MS, CPHIMs, VHA Office of Informatics and Analytics/Health Informatics
- Patricia P. Sengstack, DNP, RN-BC, FAAN, Vanderbilt University
- Hardeep Singh, MD, MPH, Michael E. DeBakey VA Medical Center and Baylor College of Medicine
- Dean Sittig, PhD, The University of Texas Health Science Center at Houston, School of Biomedical Informatics
- Paul Tang, MD, MS, IBM Watson Health

©2018 ECRI INSTITUTE
Questions? Contact hit@ecri.org
Education and Learning Opportunities

HEALTH IT USER EDUCATION

Learning Objectives

- Review the safety process
- Understand the importance of integrating health information technology (IT) into your organization’s safety program
- Identify a health IT safety event, near miss, and hazard
- Understand the process for reporting and investigating health IT safety events, near misses, and hazards in your organization
- Encourage learning from discussing and reporting of health IT–related safety events, near misses, and hazards
Framework for Integrating a Health IT Safety Program

1. Leadership and staff commitment to health IT safety
2. Define a culture of safety
3. Incorporate organizational patient safety strategy and commit resources
4. Apply improvement methods, considering human factors and reliability science

Integrating Health IT Safety

- Health IT safety does not function in a silo
- It should be incorporated into the general safety program
- It is impacted by multiple sociotechnical elements

Sprig et al. (2011)
Do you recognize when health IT might be involved in a safety event, near miss, or hazard?

- Yes
- No
- Unsure

What is a health IT–related safety event?

- A health IT–related patient safety event is any event triggered by, or related to, the technology that has caused patient harm, has the potential to cause patient harm, or that causes a delay in treatment or misdiagnosis. These errors would not occur but for the use of technology. (Carayon et al. 2012).

- A health IT–related safety event or hazard has the potential to occur anytime health IT is unavailable for use, malfunctions during use, is used incorrectly by someone, or when health IT interacts with another system component incorrectly, so that data is lost or incorrectly entered, displayed, or transmitted. (Sittig and Singh, 2011).
Are Health IT Safety Events Different from Patient Safety Events?

- Yes
- No
- Unsure

How Do You Recognize Whether Health IT Might Have Contributed to an Event?

- Did the health IT issue or event result in injury or death of a patient?
- Could the health IT issue or event potentially cause injury to a patient?
How Do You Recognize Whether Health IT Might Have Contributed to an Event?

- Did the health IT issue or event result in injury or death of a patient?
- Could the health IT issue or event potentially cause injury to a patient?

Case Examples of Health IT–Related Events

- A surgeon tried to access a patient’s radiology study from the PACS system in the OR (operating room). The display would only show a blue screen. The patient’s time under anesthesia was extended while efforts were made to get the computer display to work.
**Case Examples of Health IT–Related Events**

- The physician ordered that the patient’s anticoagulation medication be discontinued after reviewing results for the patient’s prothrombin time. This order did not cross over to the pharmacy system. Because the order was not transmitted, the patient received eight extra doses of the medication before it was finally discontinued. The IT department indicated a planned upgrade will address the problem.

- The nurse entered an incorrect patient identification number and the blood glucose results from the bedside glucose meter were recorded to the wrong patient record. The correct patient was treated because the blood glucose results were immediately available and visible at the bedside.
Items That Should Signal Health IT–Related Safety Issues

- Unexpected electronic health record (EHR)-related downtime lasting more than eight hours
- Interruptive alerts that have fired more than 100 times with a 100% override rate
- Erroneous displays of laboratory test results or medications
- Roll-back to an older version of EHR software (e.g., a software upgrade affected the system’s function)
- Instances in which a data backup failed to reload properly
- Data losses affecting more than 100 patients
- Software calculation errors affecting more than 100 patients
- System configuration errors affecting more than 100 patients

Organizational Recommendations for Increasing Health IT Safety Awareness

- Provide health IT safety training and opportunities for continuous learning—
  - For all new employees
  - Periodically for existing employees (e.g., annually, prior to upgrade, fixes, or implementation of new software)
  - As part of staff evaluations and competencies
  - With remediation provided when competencies are not met
- Reporting procedure
  - Review the organization’s procedure for reporting a health IT safety issue, event, hazard, or near miss (including reporting to vendors).
  - Identify new ways to learn about safety issues using existing techniques (e.g., safety huddles, walkrounds)
Algorithm for Health IT Patient Safety Event Process

Health IT Patient Safety Event—Steps

Refer to algorithm

- **Patient safety event reported**
  - Determine whether immediate or interim actions are needed
  - Determine whether the reported issue is related to health IT
    - Health IT-related? YES—(then follow that pathway)
    - Health IT-related? NO—(then follow the process below)
      - Determine whether technology can help to mitigate issue
      - Can technology help? If YES, go to REVIEW
      - Can technology help? If NO, determine other solution
Health IT Patient Safety Event—Steps

- Investigate health IT contributing factors
  - Considering first the sociotechnical dimensions:
    - Hardware and software
    - Clinical content
    - Human-computer interface
    - People
    - Workflow and communication
    - Policies, procedures, environment, and culture
    - External rules, regulations, and pressures
    - System measurement and monitoring

Patient Safety Event Reported, Identified, and Assessed: Part 1
Health IT Patient Safety Event—Steps

- Employ patient safety, risk, or quality; internal IT; and/or vendors to investigate, analyze, and help to identify health IT contributing factors using the reporting taxonomies

  - Consider AHRO Common Format taxonomy’s contributing factors:
    - Incompatible devices
    - Equipment/device function
    - Equipment/device maintenance
    - Hardware failure or problem
    - Network failure or problem
    - Ergonomics, including human/device interface issues
    - Security, virus, or other malware issue
    - Unexpected software design issue
    - Other

  - Consider hazard-manager taxonomy’s contributing factors:
    - Usability
    - Data quality
    - Decision support
    - Vendor factors
    - Local implementation
    - Other factors

- Collaborate: Collaborate with subject matter experts (SMEs) to determine risk score, conduct gap analysis, and assign priority to identify solutions and long-term adjustments

- Develop: Determine actions required, assign accountability, and conduct testing to ensure readiness for implementation

- Deploy: Implement appropriate fixes and provide updates to users

- Remediate: Monitor and evaluate fixes to identify any other systems that may be impacted, as well as validity of the fix moving forward

- Track: Determine whether the plan is effective
  - Action plan effective?
  - Action plan effective? If NO, return to “Develop”

- Communicate: Report learnings and create strategies for addressing findings and status to all stakeholders
Who Should Report a Health IT–related Safety Event?

- Physician
- Nurse
- Medical assistant
- Radiologist
- Technician
- Registration
- Billing
- Coders
- Pharmacist
- Anyone who uses technology that interacts with a patient
Developing, Implementing, and Integrating a Health IT Safety Program

Health IT Safety Process—ICE

Integrate
Identify ways to integrate health information technology (IT) safety into existing safety programs

Collaborate
Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety

Embed
Embed safety into the culture and daily workflow to achieve a unified vision of health IT safety

Multiple Stakeholders

Integrate, Collaborate, and Embed

- Change the culture—be proactive versus reactive
- Provide support from leadership
- Assign adequate resources to the safety program
- Work collaboratively with vendors on solutions and optimization
- Use a consistent risk/safety/hazard method
- Training/education—competency for all leadership and staff
- Resources and tools—SAFER Guides, toolkit items
- Include all technology when assessing issues: EHRs, e-prescribing, computerized provider order entry (CPOE), clinical decision support (CDS), barcoding, laboratory information systems (LIS), smart pumps, and medical devices
Tools To Aid Implementation

- SAFER Guides (ONC)
- Sentinel Event Alert 54: Safe use of health information technology (Joint Commission)
- Risk Assessment Tools (AHRQ)
- Algorithm – Health IT Issue Analysis
- Reporting tools
- Health IT Issues log
- Patient Safety Leadership WalkRounds™ (IHI)
- Safety briefings tool (IHI)
- Daily safety briefings (Joint Commission)
- AHRQ TeamSTEPPS® – Safety Huddles
- Conducting a morning briefing (AHRQ)

Tools To Aid Implementation (Cont’d)

- Health Information technology through the lens of patient safety (IHI/NPSF)
- Take 5: safe use of health information technology (Joint Commission [audio file])
- The digital transformation: how technology is helping (and hurting) healthcare IHI
- Infographic–Health IT Awareness, case examples
- AHRQ Common Formats
- Health information technology hazard manager (Pennsylvania: AHRQ)
- Health IT Issues Log/Dashboard
- Educational PowerPoint
- Checklists
References


Workgroup Members for Developing, Integrating, and Maintaining a Health IT Safety Program

Chair: Patty Sengstack, DPN, RN-BC, FAAN, Vanderbilt University
- Don Amonga, The Pew Charitable Trust
- Geoff Capka, Allscripts
- Gerard Castro, The Joint Commission
- Allen Chen, Johns Hopkins Medicine
- Andrea Cobb, Texas Medical Association
- Brian Crawford, Epic
- Mike Favreau, Allscripts
- Trisha Flanagan, athenahealth
- Roy Gill, NextGen
- Richard Hornaday, Allscripts
- T. Jamison, PAA
- Joe Lewelling, AAMI
- Trish Lugtis, constellation
- Laura Majewski, Beaumont Health System
- Wendi Mielgoz, Sutter Health System
- Mike Midgley, RN, JD, MPH ASHRM
- Divya Parikh, PAA
- Jim Russell, Epic
- Donna Summers, Henry Ford Health System
- Tim Swice, Bipartisan Policy Center
- Peli Yu, Arkansas Children’s Hospital

ECRI Institute staff:
- Ronni Solomon, JD, Executive Vice President and General Counsel
- Ellen Deutsch, MD, MS, FAAP, FACS, CPPS, Medical Director
- Robert Giannini, NHA, CMTS-IM/CP, Patient Safety Analyst and Consultant
- Patricia Guiffrida, RN, MSN, CPHIMS, Patient Safety and HIT Safety, ECRI Institute
- Amy Goldberg-Alberts, MBA, FASHRM, CPHRM Executive Director, Partnership Solutions Patient Safety, Risk, and Quality
- Scott Lucus, PhD, PE, Director, Accident and Forensic Investigation
- Jeremy J. Michel, MD, MHS, Health Technology Assessment, ECRI-Penn AHRQ Evidence Based Practice Center (EPC)
- Lorraine Passanante, DPM, JD, MBE, FACFOM, FAPWCA, Senior Patient Safety, Risk, and Quality Analyst
- Anisha Skariya, MPH, RRT
- Amy Tsoi, MD, MSc, Senior Research Analyst, Health Technology Assessment, ECRI-Penn AHRQ Evidence Based Practice Center (EPC)
Partnership Expert Advisory Panel

- David W. Bates, MD, MSc, Brigham and Women’s Hospital
- Kathleen Blake, MD, MPH, American Medical Association
- Pascale Carayon, PhD, University of Wisconsin-Madison College of Engineering
- Tejal Gandhi, MD, MPH, National Patient Safety Foundation
- Chris Lehmann, MD, Vanderbilt University Medical Center
- Peter J. Pronovost, MD, PhD, The Johns Hopkins University School of Medicine
- Jeannie Scott, MS, CPHIMS, VHA Office of Informatics and Analytics/Health Informatics
- Patricia P. Sengstack, DNP, RN-BC, FAAN, Vanderbilt University
- Hardeep Singh, MD, MPH, Michael E. DeBakey VA Medical Center and Baylor College of Medicine
- Dean Sittig, PhD, The University of Texas Health Science Center at Houston, School of Biomedical Informatics
- Paul Tang, MD, MS, IBM Watson Health

Questions? Contact hit@ecri.org
Questions? Contact hit@ecri.org
Self-Assessment Questionnaires for a Safety Culture

SAFETY CULTURE LEADERSHIP

HOW TO COMPLETE THE SURVEY

1. Role question: choose the role that best applies to your role/job position within the organization.

2. Answer the three background questions.

3. Complete the 18 multiple-choice questions in the categories of integrate, collaborate, and envision.

4. There are two optional questions allowing written comments.

The safety culture leadership survey (the SAQ) can be used in conjunction with the Health IT Safety Culture Assessment Frontline Users Scorecard and Action Plan. The scorecard and action plan tallies results from the SAQ to create a scorecard to be used to develop an action plan using ICE strategies and tools to integrate, collaborate, and embed a culture of health IT safety. An Excel version of the scorecard can be found at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/SAQ_Leadership.xls.
Role Question

1. Check one that best applies to your job/position within the organization.

- Clinical Leadership
- Non-Clinical Leadership
- Information Technology Leadership
- Support Staff Leadership
- Administrative Leadership

Background Questions

1. How many hours per week do you work in this organization? ________

2. How long have you worked for this organization?
   - a. Less than 1 year
   - b. 1 to 5 years
   - c. 6 to 10 years
   - d. 11 to 15
   - e. 16 or more years

3. At which location do you work? ______________________________

Integrate

1. Health IT safety is recognizable as high priority in the organization.
   - a. Incorporated in operations
   - b. Routinely assess and evaluate
   - c. Not presently a consideration

2. Leadership understands that an ineffective health information technology (IT) safety program can be catastrophic and will be a loss to the organization’s internal and external reputation.
   - a. Incorporated in operations
   - b. Routinely assess and evaluate
   - c. Not presently a consideration

3. The health IT safety goals are formalized in the organization’s planning and strategic documents.
   - a. Incorporated in operations
   - b. Routinely assess and evaluate
   - c. Not presently a consideration
4. The healthcare organization has developed the business case for incorporating health IT safety into the existing safety program.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. No presently a consideration

5. The healthcare organization provides adequate funding and resources needed to evaluate and upgrade technologies and processes to improve health IT safety.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

6. Health IT subject matter experts (SMEs) are included in the safety program (for example: chief nursing informatics officer [CNIO], chief medical informatics officer [CMIO], in-house IT, staff, vendors, quality, risk, performance improvement, informaticist, front-line health IT users).
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

7. A leader/champion has been identified to incorporate health IT safety into present safety efforts.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

Collaborate

8. The healthcare organization facilitates procedures for interruptions in technology or its availability that impact or have the potential to impact patient safety (e.g., ransomware, downtimes, power outages, software problems, interoperability).
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

9. The healthcare organization identifies and obtains the support of the key stakeholders from all areas where health information technology is used.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration
10. The healthcare organization and vendor/developer organizations work in collaboration to investigate health IT-related safety events, near misses, or hazards.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

11. The healthcare organization and vendor/developer organizations work in collaboration to explore ways that health IT can improve the workflow and effectiveness of clinical and nonclinical staff.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

Embed

12. There is open and transparent communication within the organization about the health IT safety programs and goals.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

13. The health IT safety risk and hazards are integrated into the organization’s risk activity assessment.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

14. The healthcare organization encourages the reporting of health IT–related safety and suspected health IT–related safety issues, events, and hazards.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

15. The healthcare organization routinely performs a health IT safety culture assessment.
   a. Incorporated in operations
   b. Routinely assess and evaluate
   c. Not presently a consideration

16. The healthcare organization addresses areas of opportunity and needed improvement identified in the health IT safety culture assessment.
   a. Incorporated in operations
b. Routinely assess and evaluate

c. Not presently a consideration

17. The healthcare organization identifies educational opportunities for leaders, staff, and patients to improve health IT safety.

a. Incorporated in operations

b. Routinely assess and evaluate

18. The healthcare organization has a comprehensive policy for monitoring hazards and potential hazards that incorporates how to respond to safety events, near misses, or hazards.

a. Incorporated in operations

b. Routinely assess and evaluate

c. Not presently a consideration

Optional questions

19. Considering health IT safety, what does your organization do well to promote a culture of health IT safety?

20. Considering health IT safety, what does your organization need to improve to promote a culture of health IT safety?
SAFETY CULTURE HEALTH IT USERS

HOW TO COMPLETE THE SURVEY

1. Role question: choose the role that best applies to your role/job position within the organization.

2. Answer the three background questions.

3. Complete the 22 multiple choice questions in the categories of integrate, collaborate, and envision using the Likert scale:
   - [ ] Strongly agree
   - [ ] Agree
   - [ ] Neither agree nor disagree
   - [ ] Disagree
   - [ ] Strongly disagree

4. There are two optional questions allowing written comments.

The safety culture health IT users survey (the SAQ) can be used in conjunction with the Health IT Safety Culture Assessment Frontline Users Scorecard and Action Plan. The scorecard and action plan tallies results from the SAQ to create a scorecard to be used to develop an action plan using ICE strategies and tools to integrate, collaborate, and embed a culture of health IT safety. An Excel version of the scorecard can be found at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/SAQ_Users.xls.
Role Question

1. Check one that best applies to your job/position within the organization.

- Nursing staff (NP, CRNA, CNS, CNM, LPN, RN)
- Medical staff (Physician, Resident, Intern, Attending, Hospitalist)
- Other clinical staff (Physician Assistant, Medical Assistant, Patient Care Tech, Patient Care Aide, Nursing Assistant, Dietician, Pharmacist, Pharmacy Technician, Physical, Occupational, or Speech Therapist, Psychologist, Respiratory Therapist, Social Worker, Technologist, EKG Technician, Phlebotomist, Radiology Technician)
- Clerical Staff (Unit Clerk, Secretary, Receptionist, Front Office Staff, Back Office Staff, Billing Staff)
- Support Staff (Facilities Staff, Food Services, Housekeeping Staff, Environmental Services, Clinical Informatics Staff, Security, Transporter)
- IT Staff (Information Technology Staff, Health Information Services Staff, Clinical Informatics)

Background questions

1. How many hours per week do you work in this organization? ________

2. How long have you worked for this organization?
   a. Less than 1 year
   b. 1 to 5 years
   c. 6 to 10 years
   d. 11 to 15 years
   e. 16 or more years

3. At which location do you work? ______________________________

Integrate

1. Health IT safety is recognizable as a top priority in this healthcare organization.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

2. Leadership delivers a clear message that failure of health IT safety can be catastrophic and will be a loss to the organization’s internal and external reputation.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree
3. We have policies and procedures that clearly address health IT safety.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

4. Adequate resources (e.g., staff, equipment, and/or time) are assigned to handle the daily workload.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

5. Health IT subject matter experts (SMEs) are included in the safety program (for example: chief nursing informatics officer [CNIO], chief medical informatics officer [CMIO], in-house IT, staff, vendors, quality, risk, performance improvement, informaticist, front-line health IT users).
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

6. A leader/champion has been identified to incorporate health IT safety into the present safety effort.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

Collaborate

7. The healthcare organization and vendors work in collaboration in investigating health IT–related patient safety events, near misses, or hazards.
   a. Strongly agree
   b. Agree
c. Neither agree nor disagree
d. Disagree
e. Strongly disagree

8. The internal IT department is involved in investigating health IT–related patient safety events, near misses, or hazards.
   a. Strongly agree
   b. Agree
c. Neither agree nor disagree
d. Disagree
e. Strongly disagree

9. Leadership communicates follow-up and updates on reported IT-related safety and suspected safety events, near misses, or hazards.
   a. Strongly agree
   b. Agree
c. Neither agree nor disagree
d. Disagree
e. Strongly disagree

10. The healthcare organization provides health IT safety training for all new staff.
    a. Strongly agree
    b. Agree
c. Neither agree nor disagree
d. Disagree
e. Strongly disagree

11. The healthcare organization periodically conducts health IT safety competency assessments for all staff.
    a. Strongly agree
    b. Agree
c. Neither agree nor disagree
d. Disagree
e. Strongly disagree
12. The healthcare organization provides training for all staff when competency is not met.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

13. We know how to identify when health IT is a factor in a safety concern, issue, event, or hazard.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

14. We recognize that technology workarounds often tell us that there is an issue that must be addressed.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

15. There is open communication within the healthcare organization about the health IT safety programs and goals.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

16. The healthcare organization periodically conducts a health IT safety culture assessment.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
17. The health care organization shares the health IT safety-culture assessment results and action plans with the staff.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

18. The healthcare organization monitors compliance with the health IT safety program’s policies and procedures.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

19. The healthcare organization incorporates the compliance information into the staff evaluations and/or clinician credentialing.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

20. The healthcare organization has a comprehensive policy for monitoring hazards and potential hazards that incorporates how to respond to health IT safety issues.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree
21. We are encouraged to report health IT–related safety and suspected health IT–related safety issues, concerns, events, near misses, or hazards.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

22. We know the process to escalate a potential safety issue to determine whether the technology played a role.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

Additional comments

23. Considering health IT safety, what does your organization do well to promote a culture of health IT safety?

24. Considering health IT safety, what does your organization need to improve to promote a culture of health IT safety?
Leadership and Organization Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan

This tool can be used to track your results from the self-assessment questionnaire (SAQ), safety culture for leadership. The scorecard and action plan tallies results from the SAQ to create a scorecard to be used to develop an action plan using ICE-strategies and tools to integrate, collaborate, and embed a culture of health information technology (IT) safety. This tool can be used as you move through the process of assessing, evaluating, and remediating the culture of health IT safety in the organization. Using a five-point Likert scale, answers are categorized as low priority or no action required (highlighted in yellow) or medium to high priority (highlighted in red). Based on the result of the self-assessment, it can also be used to record, monitor, track, and compare your results year over year. An Excel version of the scorecard can be found at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/SAQ_Leadership.xls.
Health IT Users Self-Assessment Questionnaires for a Safety Culture: Scorecard and Action Plan

This tool can be used to track your results from the self-assessment questionnaire (SAQ), safety culture for health IT users. The tool tallies results from the SAQ to create a scorecard to be used to develop an action plan using ICE-strategies and tools to integrate, collaborate, and embed a culture of health information technology (IT) safety. This tool can be used as you move through the process of assessing, evaluating, and remediating the culture of health IT safety in the organization. Using a five-point Likert scale, answers are categorized as low priority or no action required (highlighted in yellow) or medium to high priority (highlighted in red). Based on the result of the self-assessment, it can also be used to record, monitor, track, and compare your results year over year. An Excel version of the scorecard can be found at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/SAQ_Users.xls.
Health IT Dashboard

The health IT dashboard helps gather information about health IT–related safety events for tracking, trend analysis, and dissemination of data throughout the organization. It provides the opportunity to look at health IT–related events by event type (e.g., medication, laboratory, radiology), harm (hazard or patient harm), and health IT category. It also can be used to assess and track the patient-safety risk level of issues and the status of the mitigation plan. The dashboard can be accessed online at [https://www.ecri.org/HITPartnership/Resources/HIT_Safety/Dashboard.xls](https://www.ecri.org/HITPartnership/Resources/HIT_Safety/Dashboard.xls).
Health IT Safety Program Evaluation Tool

The Health IT Safety Program Evaluation Tool is used to evaluate user awareness, lack of awareness, or lack of implementation of specific factors, and the impact they have had on the success or failure of your program. The tool will help you evaluate and monitor the implementation process of your program.

Use this tool to analyze whether these factors impeded your success, had no effect, or supported your success. The results can guide you in improving your program’s implementation. An Excel version of the tool can be accessed at https://www.ecri.org/HITPartnership/Resources/HIT_Safety/Ongoing_Evaluation_Tool.xls.
HEALTH IT SAFETY PROGRAM EVALUATION TOOL

<table>
<thead>
<tr>
<th>Organizational Factors</th>
<th>Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health information technology (IT) safety is recognizable as a top priority in the organization.</td>
<td>What was the perception of this factor when you started your health IT safety program?</td>
</tr>
<tr>
<td>Leadership delivers a clear message that failure of health IT safety can be catastrophic and will be a loss to the organization’s internal and external reputation.</td>
<td>What impact did user awareness, lack of awareness, or lack of implementation of this factor have on the success of your health IT safety program?</td>
</tr>
<tr>
<td>The health IT safety goals are formalized in the organization’s planning and strategic documents.</td>
<td></td>
</tr>
<tr>
<td>The organization has developed the business case for incorporating health IT safety into the existing safety program.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization has policies and procedures that clearly address health IT safety.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization assigns adequate resources to the health IT safety program.</td>
<td></td>
</tr>
<tr>
<td>Health IT subject matter experts (SMEs) are included in the safety program (for example: chief nursing informatics officer [CNIO], chief medical informatics officer [CMIO], in-house IT, staff, vendors, quality, risk, performance improvement, informaticist, front-line health IT users).</td>
<td></td>
</tr>
<tr>
<td>A leader/champion has been identified to incorporate health IT safety into the present safety effort.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization encourages the reporting of health IT–related safety and suspected health IT–related safety events, near misses, and hazards.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization and vendors collaborate to investigate health IT–related patient safety issues.</td>
<td></td>
</tr>
<tr>
<td>Leadership communicates follow-up and updates on reported IT-related safety and suspected safety events, near misses, or hazards.</td>
<td></td>
</tr>
<tr>
<td>There is open communication within the healthcare organization about the health IT safety programs and goals.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization provides health IT safety training for all new staff.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization periodically conducts health IT safety competency assessments for all staff.</td>
<td></td>
</tr>
<tr>
<td>The healthcare organization incorporates the information into the staff evaluations and/or clinician credentialing.</td>
<td></td>
</tr>
<tr>
<td>The health IT safety risk and hazards are integrated into the organization’s risk activity assessment.</td>
<td></td>
</tr>
</tbody>
</table>
Communication and Transparency Tools for a Health IT Safety Program

The following tools can be used to incorporate transparency into the health IT safety program by providing methods for feedback and communication:

- Banners at log-on to the software and/or application
- Newsletters, highlights of events (include near misses and provide data)
- Email alerts
- Safety memo (see following)
- Safety report feedback log (see following)
COMMUNICATION TOOL: SAMPLE SAFETY MEMO
(Insert your organization’s logo)

SAFETY ISSUE MEMO

Date:

Issue:
Include brief description of event, near miss, or hazard

Who needs this information?
User role

What users need to know?
Include details of:
• Event, near miss, or hazard
• Applications affected
• Screen shots, charts
• Action plan

What users need to do?
New workflow to avoid a recurrence of the event, near miss, or hazard

Resolution:
Communicate to users when the issue is resolved
COMMUNICATION TOOL: SAMPLE SAFETY REPORT FEEDBACK LOG
(Insert your organization’s logo)

SAFETY EVENT, NEAR MISS, OR HAZARD REPORT FEEDBACK LOG

Event Report Date:

To Reporter:

Event Report Description:

Review and Action Plan:
Resolved:

| YES | NO | PENDING |

Resolution:

Communicated to Reporter From:

| YES | NO |
Appendix

ADDITIONAL RESOURCES


Agency for Healthcare Research and Quality (AHRQ):


Association for the Advancement of Medical Instrumentation:


Healthcare Information Management System Society (HIMSS):


Institute for Healthcare Improvement (IHI):


The Joint Commission:


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


