Integrating a Health IT Safety Program

Recommendations & Implementation Strategies
Recommendations & Implementation Strategies

Integrating a Health IT Safety Program
Acknowledgments

We would like to thank workgroup chair, Dr. Patricia Sengstack, and the workgroup participants for their contributions. The recommendations and implementation strategies identified in the Safe Practice Recommendations for Developing, Implementing, and Integrating a Health IT Safety Program toolkit were conceived and developed by the following workgroup participants and contributors:

Workgroup Chair
Patricia P. Sengstack, DPN, RN-BC, CPHIMS, FAAN, Vanderbilt University Medical Center

Workgroup Members
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 and Pediatrics, and Health IT Patient Safety Officer, 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 Hornaday, Senior Solutions Manager—Public Health and Certification, Allscripts
T. Jamison, Medical Professional Liability Association
Joe Lewelling, Vice President, Emerging Technologies and Health IT, Association for the Advancement of Medical Instrumentation
Trish Lugtu, CPHIMS, Senior Manager, Advanced Analytics Solutions, Constellation
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

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

ECRI Institute Internal Partnership Contributors
Ronni Solomon, JD, Executive Vice President, Chief Policy and External Affairs Officer
Asa Adadey, MS, Database Analyst
Julia L. Barnedt, MA, Editor
Robert C. Giannini, NHA, CHTS-IM/CP, Patient Safety Analyst and Consultant
Patricia Giuffrida, MSN, RN, CPHIMS, Senior Patient Safety and Health IT Safety Analyst
Amy Goldberg-Alberts, MBA, FASHRM, CPHRM, Executive Director, Patient Safety, Risk, and Quality
Tara Kolb, Manager, Media Services
Ben Pauldine, MBA, Senior Graphic Designer
Lorraine Possanza, DPM, JD, MBE, FACFOAM, Program Director, Partnership for Health IT Patient Safety
Amy Tsou, MD, MSc, Associate Medical Director, ECRI Institute—Penn Medicine Evidence-based Practice Center
Amelia Vagnozzi, MHA, BSN, RN, CNOR, Clinical Healthcare Informaticist
Diana Winters, Copyeditor
Andrea Zavod, Managing Editor

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 K. Gandhi, MD, MPH, CPPS, Institute for Healthcare Improvement
Christoph U. Lehmann, MD, FAAN, FACMI, FIAHSI, Vanderbilt University Medical Center
Peter J. Pronovost, MD, PhD, University Hospitals
Daniel J. Ross, MD, DDS, Department of Defense, Defense Health Agency
Jeanie Scott, MS, CPHIMS, Veterans Health Administration, Office of Informatics and Analytics/Health Informatics
Patricia P. Sengstack, DNP, RN-BC, CPHIMS, FAAN, Vanderbilt University Medical Center
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
Introduction

Health information technology (IT) is integral to healthcare today. Health IT safety in some ways is like an iceberg, with the bulk of the potential safety risks, as well as the new potential safety uses, remaining uncovered.

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, cultural readiness, installation and implementation practices, workflow, training, handling of upgrades, and continued innovation. Improving safety requires attention to all of these areas.\(^1\) With this in mind, the Partnership focused on developing recommendations for integrating, collaborating, and embedding health IT safety into an organization’s safety strategy. The goal—to prevent the silo effect of addressing health IT issues in isolation.

Overview

To facilitate development and integration of a health IT safety program, the Partnership convened a multistakeholder workgroup to evaluate processes and practices for incorporating health IT safety into a general safety program. This work was informed by synergies realized by combining subject matter experts (researchers, IT professionals, clinicians, healthcare organizations, vendor/developers, and professional organizations), relevant information (expert examples of health IT safety programs), and perspectives with the Partnership’s evidence and event analysis available from ECRI Institute PSO in its role as a federally qualified Patient Safety Organization (PSO).

The recommendations incorporate enterprise risk management techniques, consider the sociotechnical model, and advance and expand the development of a safety culture to include a health IT safety culture. Anticipating and mitigating the unintended consequences of developing and using health IT throughout its lifecycle is the focus of a health IT safety program. The safe practice recommendations and implementation strategies for developing, implementing, and integrating a health IT safety program are addressed here and are intended as a resource for all stakeholders including clinicians, IT professionals, safety leaders, vendors and developers, regulators, and patients. This guide will help with the implementation of those recommendations.
Recommendations

Integrate: Identify ways to integrate health information technology 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

The Partnership continues to emphasize that health IT safety is a shared responsibility that should not exist in organizational silos. As such, it is important to deploy risk and mitigation strategies while incorporating health IT into the organization’s safety plan and culture. While health IT safety risks may not be readily apparent or clearly identified and reported, learnings obtained by recognizing their significance to a risk and safety program will create awareness so these learnings can function as the building blocks for integrating, collaborating, and embedding health IT safety efforts. This work provides tools to facilitate incorporating the domains of health IT safety; safe health IT, safe use of health IT, and use of health IT for safety; into a safety program. Additional information and tools are available in the full report.
Integrate: Identify ways to integrate health information technology safety into existing safety programs

**Rationale:** 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 health IT issues and concerns and identifying new ways that health IT promotes safety is the primary reason for integrating health IT into a safety program.

**What is technology’s role?**
Develop and implement a reporting technology platform that facilitates communication to all appropriate stakeholders from issue identification through resolution. Incorporate technology for simulated learning; self-assessments; or to update users of changes in the system including upgrades, updates, or other modifications.

**What can stakeholders do?**
It is important that stakeholders recognize ongoing safety concerns. Learning to recognize issues and potential issues and communicating them with peers and colleagues is an important first step. By incorporating health IT safety into an organization’s general safety program and using the safety program principles, stakeholders can identify and mitigate risks.

**How can this be done?**
- Obtain leadership commitment and support
- Clearly define what a health IT-related patient safety event is; what it can be triggered by, or related to; and how it potentially can cause patient harm, delay care, or impact an organization’s reputation
- Providing appropriate training and continuous learning about the triple aim of safe technology, safe use of technology, and the use of technology for safety
- Inform staff when new technologies are added, or when upgrades or replacements occur (staff may have been using a workaround that will be impacted by such modifications)
- Share use cases that highlight health IT-related issues, concerns, and unintended consequences when conducting education or raising awareness
- Encourage reporting of known or suspected health-IT related safety issues
- Measure and evaluate the effectiveness of the risk strategies that are used, and match performance metrics to clinically relevant measures to shed light on effective safety efforts (e.g., metrics on downtime, uptime, alert overrides, system response times, open orders, number of clicks)
Table 1. How Stakeholders Can Integrate Health IT into Existing Safety Programs

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clinicians</strong></td>
<td>Use the following General Safety principles to integrate health IT technology into existing safety programs:</td>
</tr>
<tr>
<td></td>
<td>- Risk identification:</td>
</tr>
<tr>
<td></td>
<td>◦ Use both proactive (e.g., failure modes, safety assessments, awareness studies) and reactive (e.g., investigations, root-cause analyses [RCAs], common cause analysis) strategies for advancing safety and safety issues</td>
</tr>
<tr>
<td></td>
<td>◦ Integrate identifying and reporting health IT–related risk into risk assessments and activities</td>
</tr>
<tr>
<td></td>
<td>- Risk analysis/assessment:</td>
</tr>
<tr>
<td></td>
<td>◦ Assess for safety before introducing new technology and/or upgrades (e.g., test scripts, use-case testing, information flow evaluations, simulation)</td>
</tr>
<tr>
<td></td>
<td>◦ Encourage reporting (e.g., patient safety organization [PSO], IT, vendor/developers) within the organization</td>
</tr>
<tr>
<td></td>
<td>◦ Ensure active participation by health IT subject matter experts (SMEs) in organizational safety meetings, investigations, analysis, resolutions, and uses of technology for safety</td>
</tr>
<tr>
<td></td>
<td>- Risk mitigation:</td>
</tr>
<tr>
<td></td>
<td>◦ Incorporate health IT safety into enterprise risk strategies</td>
</tr>
<tr>
<td></td>
<td>◦ Encourage reporting (PSOs, IT, vendor/developers, others)</td>
</tr>
<tr>
<td></td>
<td>◦ Implement vendor/developer recommendations to avoid internal workarounds</td>
</tr>
<tr>
<td></td>
<td>◦ Create a health IT–related reporting system with a common reporting language</td>
</tr>
<tr>
<td></td>
<td>◦ Use walkarounds, safety huddles, and summaries to identify and report issues for action</td>
</tr>
<tr>
<td></td>
<td>- Risk control:</td>
</tr>
<tr>
<td></td>
<td>◦ Test and monitor implementations, upgrades, and modifications as appropriate across the technology’s lifecycle</td>
</tr>
<tr>
<td></td>
<td>◦ Report health IT–related patient safety events to vendor/developers, PSOs, organizational staff</td>
</tr>
<tr>
<td></td>
<td>◦ Identify and implement safety standards</td>
</tr>
<tr>
<td></td>
<td>◦ Employ continuous reporting, tracking, and transparency (reporting back) for issue resolution</td>
</tr>
<tr>
<td></td>
<td>- Risk assumption:</td>
</tr>
<tr>
<td></td>
<td>◦ Develop a health IT–related analysis process for events</td>
</tr>
<tr>
<td></td>
<td>◦ Develop metrics for health IT assessments and outcomes</td>
</tr>
<tr>
<td><strong>Healthcare organizations</strong></td>
<td>Readily communicate health IT-related safety concerns, issues, event, errors, near misses, or hazards to clients and internal departments</td>
</tr>
<tr>
<td></td>
<td>Be receptive to safety concerns, issues, events, errors, near misses, or hazards reported by clients, and act on them in timely manner</td>
</tr>
<tr>
<td></td>
<td>Provide end-users with opportunities to participate in the design and testing of software</td>
</tr>
<tr>
<td></td>
<td>Ensure that everyone in the developer organization knows how to internally report a safety concern to drive further action</td>
</tr>
<tr>
<td></td>
<td>Promote and commit to a health IT safety program that encourages reporting and open discussion of safety concerns in a nonpunitive environment</td>
</tr>
<tr>
<td><strong>Vendors/developers</strong></td>
<td>Generate awareness that unreported or underreported health IT-related safety events can lead to patient harm</td>
</tr>
<tr>
<td></td>
<td>Acknowledge that safe health IT, the safe use of health IT, and using health IT safely is the responsibility of all clinicians and healthcare organizations²</td>
</tr>
<tr>
<td></td>
<td>Promote and commit to a health IT safety program that encourages reporting and open discussion of safety concerns, issues, events, near misses, or known hazards in a nonpunitive environment</td>
</tr>
<tr>
<td><strong>Clinicians</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Healthcare organizations</strong></td>
<td></td>
</tr>
</tbody>
</table>
Collaborate: Convene the necessary stakeholders, including users, vendors, organizations, and patients to actively collaborate on safety

**Rationale:** 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. Included in this group are the vendor/developers, information technology experts and staff, and those clinicians not only using the technology but expert in addressing risks and benefits of using technology for safety. These collaborations support and encourage a continuous learning environment focused on safety.

**What is technology’s role?**
Use the technology to involve all members of an organization in health IT safety efforts, including leadership, staff, and others using or impacted by the use of technology. Include the technology as part of any multistakeholder analysis via assessments, reports, and measures.

**What can stakeholders do?**
To incorporate health IT effectively, those developing and working with technology and software must be included as members of existing safety program teams and actively engage in health IT-related safety initiatives. Stakeholders should convene cross-functional multidisciplinary teams to prevent the silo effect of addressing health IT-related issues in isolation. These collaborations will allow each discipline an opportunity to share their perspective and contribute their distinct knowledge for the detection, analysis, and mitigation of health IT safety risks. It is important that stakeholders proactively address safety by ensuring that health IT is in itself safe, ensuring that health IT is used safely, and identifying ways that the technology can be used to facilitate safety.

**How can this be done?**
- Provide stakeholders with training in core terminology and methods related to safe use of health IT
- Strengthen stakeholder relationships and improve collaboration by using tools that increase transparency and facilitate analysis and learning
- Promote and disseminate shared learnings of health IT safety-related best practices
- Communicate to inform action using walkarounds, daily safety huddles, and routine assessments of daily activities
- Share learnings and disseminate safety practices to all stakeholders
Table 2. How Organizations Can Convene Necessary Stakeholders to Collaborate on Health IT Safety

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Healthcare organizations | ▪ Enable continuous learning:  
                         ▪ Provide employee training and periodic updates for competency-based learning and sharing of information about health IT–related safety issues  
                         ▪ Strengthen collaborative relationships (clinician/vendor) so issues are appropriately escalated and resolved  
                         ▪ Identify and involve the appropriate parties to address and resolve safety issues  
                         ▪ Participate in multistakeholder analysis and development activities  
                         ▪ Conduct health IT simulations that represent simple and complex processes and workflows  
                         ▪ Provide learnings about health IT–related issues and hazards; share successes that have been accomplished  
                         ▪ Develop portals and information exchanges  
                         ▪ Develop checklists and assessments:  
                         ▪ Gather information and raise awareness via regularly scheduled activities (e.g., leadership walkarounds)  
                         ▪ Incorporate health IT safety, such as events and guidance, into work assessments  
                         ▪ Encourage staff participation in safety initiatives  
                         ▪ Include patient and family participation, as appropriate, encouraging their input into safety systems and checks  |
| Vendors/developers   | ▪ Use healthcare organization’s portal and information exchange  
                         ▪ Attend health IT safety training classes when scheduled, and review periodic update information when shared  |
| Clinicians          | ▪ Use patient portal and information exchanges  
                         ▪ Report issues to the site where the issue was experienced  |
| Patients/families   | ▪ Use patient portal and information exchanges  
                         ▪ Report issues to the site where the issue was experienced  |
Embed: Embed safety into the culture and daily workflow to achieve a unified vision of health IT safety

Rationale: Health IT is now widely used in healthcare with the potential to enhance and facilitate safety. However, cautions are essential when embedding technology into complex systems. When health IT safety activities are embedded into an organization’s safety culture, it is possible to prioritize risks; recognize the benefits of health IT; and enable a nonpunitive, transparent learning environment.

What is technology’s role?
Use technology to promote safety and increase transparency by providing safety dashboards, safety metrics, routine reporting, follow-up, and updates to those interacting with the technologies.

What can stakeholders do?
Vendors, developers, and those who implement, maintain, and support health IT must ensure that the technology is safe, that it is used safely, and employed to promote safety. One way this can be accomplished is to assess and embed safety into an organization’s culture and daily workflow by sharing the value of safety, changing behaviors to achieve safety goals, and employing safety strategies.

How can this be done?
- Obtain leadership commitment to safety
- Provide safety dashboards and tools to visualize progress
- Ensure a nonpunitive, just culture
- Encourage reporting and provide feedback
- Demonstrate that safety is a priority by assessing and strengthening the culture of safety
<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Healthcare organizations</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continually evaluate safety:</td>
</tr>
<tr>
<td></td>
<td>— Identify current safety awareness through self-assessments and surveys</td>
</tr>
<tr>
<td></td>
<td>— Implement survey-specific improvement strategies and monitor results</td>
</tr>
<tr>
<td></td>
<td>Foster daily workflow safety practices:</td>
</tr>
<tr>
<td></td>
<td>— Encourage increased transparency (dashboards, follow-up information, and safety updates to staff)</td>
</tr>
<tr>
<td></td>
<td>— Share survey results and conduct periodic updates to monitor status</td>
</tr>
<tr>
<td></td>
<td>— Implement safety huddles/briefings</td>
</tr>
<tr>
<td></td>
<td>Develop a just culture for safety:</td>
</tr>
<tr>
<td></td>
<td>— Create a nonpunitive culture that encourages reporting and open discussion of safety concerns and issues</td>
</tr>
<tr>
<td></td>
<td>— Identify transparent safety systems with accountability, consequences, and acknowledgements</td>
</tr>
<tr>
<td></td>
<td>— Integrate safety into the culture rather than counting on one particular leader or individual</td>
</tr>
<tr>
<td></td>
<td>— Assess health IT as part of the safety culture</td>
</tr>
<tr>
<td><strong>Clinicians</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encourage increased transparency (dashboards, follow-up information, and safety updates to colleagues and support staff)</td>
</tr>
<tr>
<td></td>
<td>Implement safety huddles/briefings</td>
</tr>
<tr>
<td><strong>Vendors/developers</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assess and evaluate technologies throughout the lifecycle</td>
</tr>
<tr>
<td></td>
<td>Continually evaluate safety:</td>
</tr>
<tr>
<td></td>
<td>— Identify current safety awareness through self-assessments and surveys</td>
</tr>
<tr>
<td></td>
<td>— Implement survey-specific improvement strategies and monitor results</td>
</tr>
<tr>
<td></td>
<td>— Implement safety huddles/briefings</td>
</tr>
<tr>
<td></td>
<td>Develop a just culture for safety:</td>
</tr>
<tr>
<td></td>
<td>— Create a nonpunitive culture that encourages reporting and open discussion of safety concerns and issues</td>
</tr>
<tr>
<td></td>
<td>— Identify transparent safety systems with accountability, consequences, and acknowledgements</td>
</tr>
<tr>
<td></td>
<td>— Integrate safety into the organization’s culture rather than counting on one particular leader or individual</td>
</tr>
</tbody>
</table>
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.² Widespread use of and reliance on health IT makes it even more important to understand both the risks and the benefits of technology.

The Partnership for Health IT Patient Safety examined ways to develop, implement, and integrate an effective health IT safety program in both healthcare and vendor/developer organizations using sociotechnical and risk models. It is time that all stakeholders 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 the technology will result.

You can access the full complement of materials at hitsafety.org or at www.ecri.org/safepractices.
References


About ECRI Institute and the
Partnership for Health IT Patient Safety

ECRI Institute is an independent, nonprofit organization improving the safety, quality, and cost effectiveness of care across all healthcare settings. The combination of evidence-based research, medical device testing, and knowledge of patient safety makes ECRI uniquely respected by healthcare leaders and agencies worldwide. For more than 50 years, ECRI Institute has had an unwavering dedication to transparency and strict conflict-of-interest policies. The organization has earned a reputation as the trusted voice of unbiased, research-based assurance for tens of thousands of members around the world using its solutions to minimize risk and improve patient care.

ECRI Institute has the only medical device testing labs in North America and the Asia Pacific where engineers conduct hands-on independent device testing for safety and human factors usability. ECRI Institute is designated an Evidence-based Practice Center by the U.S. Agency for Healthcare Research and Quality. ECRI Institute PSO is listed as a federally certified Patient Safety Organization by the U.S. Department of Health and Human Services. Visit ecri.org and follow @ECRI_Institute to learn more.

In 2013, ECRI Institute convened the Partnership for Health IT Patient Safety (Partnership), in part because of ECRI Institute’s long history of cutting-edge patient safety initiatives, and in part, in response to the growth in recognition that action was needed not only to fully realize the benefits of health information technology, but to involve the appropriate parties in the identification, classification, aggregation, analysis, and development of solutions to the ever-increasing concerns attributed to health information technology. The Partnership was established to make healthcare safer by understanding and mitigating health IT hazards and safety events. For more information on the Partnership, please visit our website.
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