PARTNERSHIP *for*
HEALTH IT PATIENT SAFETY
Making healthcare safer together

Partnering for Success

Proceedings from the
September 23, 2014 meeting
convened by ECRI Institute

Sponsored by
the Jayne Koskinas Ted Giovanis
Foundation for Health and Policy

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Forward

These Proceedings, as well as other materials on the *Partnership for Health IT Patient Safety*, can be found at http://www.ecri.org/resource-center/Pages/HITPartnership.aspx. Since publication of these Proceedings, the *Partnership* has convened a topic-specific workgroup, issued videos, disseminated case studies and newsletters, and participated in several forums. For more information, contact hit@ecri.org.

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Jayne Koskinas Ted Giovanis | Foundation for Health and Policy

ECRI INSTITUTE

Jeffrey C. Lerner, PhD
President and Chief Executive Officer

Ronni P. Solomon, JD
Executive Vice President and General Counsel

Anthony J. Montagnolo, MS
Chief Operating Officer

Vivian H. Coates, MBA
Vice President, Information Services and Health Technology Assessment

Leah Addis, MA, CPASRM
Risk Management Analyst

Paul A. Anderson
Director, Risk Management Publications

John Clarke, MD, FACS
Medical Director

Maura Crossen-Luba, MPH, CPH
Business Development Analyst/ Patient Safety Analyst

Ellen Deutsch, MD, MS, FAAP, FACS
Medical Director

Amy Goldberg-Alberts, MBA, FASHRM, CPHRM
Executive Director, Partnership Solutions Patient Safety, Risk, and Quality

Sara Goldstein, JD

Robert Giannini, NHA, CHTS-IM/CP
Patient Safety Analyst and Consultant

James P. Keller, MS
Vice President, Health Technology, Evaluation, and Safety

Tara Kolb
Manager, Media Services

William Marella, MBA
Executive Director, PSO Operations and Analytics

David Mayer, PhD
On assignment from NTSB

Laurie Menyo
Director, Public Relations and Marketing Communications

Benjamin Pauldine
Graphic Designer

Amy Poplinski
Senior Marketing Communication Specialist

Lorraine Possanza, DPM, JD, MBE, FACFOAM, FAPWCA
Senior Patient Safety, Risk, and Quality Analyst

Barbara C. Rebold, RN, MS, CPHQ
Director, Engagement and Improvement

Erin Sparnon, MEng
Engineering Manager

Cynthia Wallace, CPHRM
Senior Risk Management Analyst

Michael Wroblewski
Video Production/Design Specialist

Andrea Zavod
Managing Editor

Karen Zimmer, MD, MPH, FAAP

JAYNE KOSKINAS TED GIOVANIS FOUNDATION FOR HEALTH AND POLICY

Theodore Giovanis, FHFMA, MBA
President and Founder

J. Graham Atkinson, D.Phil.
Director

PARTNERSHIP *for*
HEALTH IT PATIENT SAFETY
Making healthcare safer together

Partnering for Success

Proceedings from the
September 23, 2014 meeting
convened by ECRI Institute

Sponsored by
the Jayne Koskinas Ted Giovanis
Foundation for Health and Policy

ECRI Institute
The Discipline of Science. The Integrity of Independence.

PARTNERSHIP *for*
HEALTH IT PATIENT SAFETY
Making healthcare safer together

Acknowledgments

THE PARTNERSHIP FOR HEALTH IT PATIENT SAFETY EXPERT ADVISORY PANEL

David W. Bates, MD, MSc
Pascale Carayon, PhD
Tejal Gandhi, MD, MPH
Terhilda Garrido, MPH, ELP
Omar Hasan, MBBS, MPH
Christopher Lehmann, MD
Peter Pronovost, MD, PhD
Jeanie Scott, CPHIMS
Hardeep Singh, MD, MPH
Dean Sittig, PhD
Paul Tang, MD, MS

ORGANIZATIONS WORKING TOGETHER WITH THE *PARTNERSHIP*

Special thanks to our participating providers. We also recognize all of the healthcare facilities participating in the *Partnership* but we are not recognizing them by name to avoid inadvertent disclosure of patient safety work product.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Table of Contents

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Partnering for Success: A Call to Action

Dear Colleagues:

In 2013, ECRI Institute convened the *Partnership for Health IT Patient Safety*, a multi-stakeholder collaborative whose purpose is to make health information technology (IT) safer together. In the short time since, the *Partnership* has become the focal point for the collaborative efforts of many groups, including healthcare providers, health IT developers, academic researchers, patient safety organizations, and professional societies. Together, we are working to share, aggregate, and analyze health IT safety data; to disseminate our findings and spread best practices; and to educate stakeholders and the broader healthcare community. The *Partnership* emphasizes learning, not enforcement. Through creation of this communal learning environment, we aim to accelerate the development of best practices and embark on improvement initiatives.

Why was the *Partnership* convened? The rapid proliferation of health IT raises the need to better understand health IT-related patient safety issues. There has been broad recognition that attention to safety is desperately needed: the Institute of Medicine, the Office of the National Coordinator for Health Information Technology, and the Bipartisan Policy Center have examined the need and recommended ways to ensure a national framework for safety. The Agency for Healthcare Research and Quality has developed Common Formats for reporting health IT-related safety issues and funded research projects on health IT safety. The Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012 directed the secretary of health and human services, acting through FDA, ONC, and FCC, to develop a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework for health IT. That draft report was issued in April 2014 with recommendations for safety. ECRI Institute's research and publications support the need for better safety data and better safety solutions.

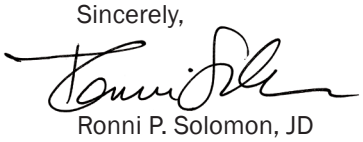
By collecting, analyzing, and sharing information, the *Partnership* will help to inform the national strategy for health IT patient safety. It's not just about looking at the unintended consequences of health IT; it is also about the powerful opportunities for using health IT to contribute to and make positive improvements in patient safety.

These Proceedings cover the health IT topics, challenges, barriers, and priorities that emerged at the *Partnership*'s September 23, 2014 meeting, Partnering for Success. The meeting underscored that health IT safety and innovation are shared responsibilities and focused on ways to advance safety through collaboration. We had a packed agenda and a stellar group of participants.

We invite you to read these Proceedings and use them in your own safety work. We are deeply grateful to all of the participants, expert advisors, and collaborating organizations that believe in the need for the *Partnership* and agreed to actively participate.

Please let us know if these Proceedings have been helpful. We look forward to hearing your suggestions and to strengthening the *Partnership*.

Sincerely,



Ronni P. Solomon, JD
Executive Vice President
General Counsel

PARTNERSHIP *for*
HEALTH IT PATIENT SAFETY
Making healthcare safer together

About the *Partnership*

The *Partnership for Health IT Patient Safety*, a private sector initiative, aims to make health information technology (IT) safer through a collaborative multi-stakeholder effort. Convened by ECRI Institute PSO, the *Partnership* leverages the work of multiple patient safety organizations (PSOs), healthcare providers healthcare provider organizations, health IT vendors, the Expert Advisory Panel, and numerous professional societies and organizations to create a learning environment that mitigates risk and facilitates improvement. It activates recommendations from the Institute of Medicine, the Office of the National Coordinator for Health Information Technology, the Bipartisan Policy Center, and the draft *FDASIA Health IT Report* by engaging stakeholders to exchange data on health IT safety issues and identify opportunities for improvement. The *Partnership* has no regulatory or enforcement powers; rather, it seeks to establish a nonpunitive learning environment in which to share and learn from health IT-related adverse events, near misses, and hazards, as well as to use health IT to provide enhanced quality care.

In order to fulfill these goals, the *Partnership* will do the following:

- Establish a nonpunitive environment for sharing and learning
- Collect, aggregate, and analyze health IT-related events, hazards, and near misses from different sources
- Identify and share promising solutions and best practices
- Inform policymakers and the broader healthcare community about the barriers and challenges associated with building a safety system for health IT and, eventually, a center for health IT safety

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Meeting Agenda

PARTNERSHIP FOR HEALTH IT PATIENT SAFETY
SEPTEMBER 23, 2014

Welcome and Overview —Ronni Solomon, JD; Jeffrey C. Lerner, PhD —Ted Giovanis, FHFMA, MBA	8:20am - 8:35am
Moderator —Janet Marchibroda, MBA	8:35am - 8:45am
Discussion Forum: What Is an "HIT Event" —David Bates, MD, MSc	8:45am - 9:30am
Discussion Forum: Classifying HIT Events —Hardeep Singh, MD, MPH; Dean Sittig, PhD	9:30am - 10:15am
Break	10:15am - 10:30am
Identifying, Triaging and Investigating HIT Safety Issues —Terhilda Garrido, MPH, ELP	10:30am - 10:45am
Breakout Groups	10:45am - 11:45am
Share Best Practices	11:45am - 12:30pm
Networking Lunch, ECRI Institute Tour	
Stakeholder Panel: How Do We Build a Learning Environment? What Does Success Look Like? —Tejal Gandhi, MD, MPH	1:30pm - 2:20pm
Stakeholder Panelists Omar Hasan, MBBS, MPH, MS, FACP (Collaborating Organization) Jeanie Scott, CPHIMS (EAP representative) Marian Dwyer, RN, MA, CPHRM, ARM (PSO representative) Carrie Tuskey, RN, MHSA (Provider representative) Sheryl Dyner (Vendor representative)	
Collaborating on Safety: Lessons from Another Industry —David Mayer, PhD	2:20pm - 2:30pm
Wrap-Up —Janet Marchibroda, MBA	2:30pm - 2:45pm
Next Steps and Adjourn	2:45pm - 3:00pm

DESIRED OUTCOMES

- Agree on the types of reports to share with the *Partnership*
- Work on ways to categorize health IT safety events and hazards
- Agree on characteristics of a successful health IT safety identification, triage, and investigation system
- Inform the national strategy for health IT patient safety
- Understand the barriers and challenges of the health IT learning system
- List practical ways in which stakeholders can immediately advance health IT safety
- Share tools and best practices
- Commit to *Partnership* goals and participate in follow-up work

Sponsored by
The Jayne Koskinas Ted Giovanis Foundation for Health and Policy

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

About Our Speakers

Jeffrey C. Lerner, PhD

Lerner has served as President and Chief Executive Officer of ECRI Institute since 2001. Prior to this, he held the position of Vice President for Strategic Planning for 17 years. He is currently serving on the Advisory Board of the U.S. Cochrane Collaboration Center.

Janet Marchibroda, MBA

Marchibroda is the director of the Health Innovation Initiative and the Executive Director of the CEO Council on Health and Innovation at the Bipartisan Policy Center, following two years serving as the chair of the Bipartisan Policy Center's Health IT Initiative. Marchibroda is also a Board Member and the initial Executive Director for Doctors Helping Doctors Transform Health Care.

Ronni P. Solomon, JD

Solomon serves as the Executive Vice President and General Counsel for ECRI Institute. She has developed and led many ECRI Institute initiatives and programs for the public and private sectors on patient safety and quality of care.

David W. Bates, MD, MSc

Bates is Senior Vice President for Quality and Safety, and Chief Quality Officer for both Brigham and Women's Hospital and Brigham and Women's Physician Organization. He is also Chief of the Division of General Internal Medicine and Primary Care at Brigham and Women's Hospital, Professor of Health Policy and Management at Harvard School of Public Health, and Co-Director of the Program in Clinical Effectiveness. Bates is also Medical Director of Clinical and Quality Analysis, Information Systems, for Partners Healthcare System. He is the chair of the Food and Drug Administration Safety Innovation Act (FDASIA) Workgroup.

Theodore Giovanis, FHFMA, MBA

Giovanis is the President and Founder of the Jayne Koskinas Ted Giovanis Foundation for Health and Policy. He has been involved in the development of many Medicare regulatory and legislative policy changes.

Hardeep Singh, MD, MPH

Singh is Chief of the Health Policy, Quality, and Informatics program at the Houston Veterans Affairs Center for Innovations in Quality, Effectiveness, and Safety, and Associate Professor of Medicine at Baylor College of Medicine. His multidisciplinary research focuses on patient safety improvement in electronic health record-based clinical settings. Singh is a member of the Clinical Laboratory Improvement Advisory Committee. He is a recipient of the 2012 Alice S. Hersh New Investigator Award for high-impact research of international significance. He received the Presidential Early Career Award for Scientists and Engineers in 2014.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Dean Sittig, PhD

Sittig is a Professor at the University of Texas School of Biomedical Informatics. He is currently serving on the American Medical Informatics Association Board of Directors and is a member of the UT-Memorial Hermann Center for Healthcare Quality and Safety. Sittig's research focuses on the design, development, implementation, and evaluation of clinical information systems.

Tejal Gandhi, MD, MPH, CPPS

Gandhi is President of the National Patient Safety Foundation and the Lucian Leape Institute. She was formerly the Executive Director of Quality and Safety at Brigham and Women's Hospital and Chief Quality and Safety Officer at Partners Healthcare. Gandhi is also an Associate Professor of Medicine at Harvard Medical School, and she is a Certified Professional in Patient Safety.

David Mayer, PhD

Mayer was the Managing Director/ Chief Operating Officer of the National Transportation Safety Board (NTSB). He was responsible for more than 50 major investigations of high-profile transportation accidents. He developed the NTSB's standardized evidence-handling procedures, which ensure that evidence is safeguarded to ensure evidentiary integrity. Mayer led U.S. participation on an International Civil Aeronautical Organization task force on protecting aviation safety information. In December 2014, Mayer became the first chief safety officer of the New York Metropolitan Transportation Authority (MTA).

Terhilda Garrido, MPH, ELP

Garrido is Vice President, HIT Transformation & Analytics in National Quality at Kaiser Permanente. She served on the Institute of Medicine committee on Health IT and Patient Safety. Her focus is in creating a patient-centered care delivery system with health information technology.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Partnering for Success

On September 23, 2014, ECRI Institute, with funding from the Jayne Koskinas Ted Giovanis Foundation for Health and Policy, convened an interactive, multi-stakeholder meeting, Partnering for Success, the first of a series of in-person meetings of the *Partnership for Health IT Patient Safety*.

Specifically, the Partnering for Success meeting was organized to address eight goals:

1. Understand the barriers and challenges of the health information technology (IT) learning system
2. Work on ways to define and categorize health IT safety issues and hazards
3. Agree on the health IT issues to share with the *Partnership*
4. Agree on characteristics of a successful health IT safety identification, triage, and investigation system
5. List practical ways in which stakeholders can immediately advance health IT safety
6. Share tools and best practices
7. Commit to *Partnership* goals and participate in follow-up work
8. Inform the national strategy for health IT patient safety

"What we have is an opportunity to really work together," said Jeffrey C. Lerner, PhD, when welcoming participants to the meeting (see "About Our Speakers" for more information on Partnering for Success presenters). "If we're able to cooperate effectively, we can work in a way that actually ensures patient safety."

Ronni P. Solomon, JD, described the purpose of the *Partnership*. "We want to make healthcare safer together," she said, through establishing a nonpunitive learning environment. Solomon emphasized the importance of working together with fellow *Partnership* participants. "We're also testing a collaborative model," she explained. "We want to achieve robust stakeholder engagement."

The work of the *Partnership* encompasses three phases:

1. **Data collection**. Data collection and aggregation across multiple organizations is crucial. The *Partnership* collects reports of adverse events, near misses, and unsafe conditions using standardized formats as well as nonstandardized data, such as alerts, help desk logs, and claims information. The data provides a foundation for *Partnership* efforts by revealing contributing factors associated with health IT–related safety issues and by identifying opportunities to use health IT to enhance patient safety. For example, usability, interoperability, and hardware/software were three topics addressed by the multi-stakeholder participants during the interactive breakout sessions. During these sessions, participants were able to share their experiences and solutions and emphasize the importance of gathering this information in a central location.
2. **Analysis**. Analysis of the information obtained from the data will facilitate improvements in patient safety and in the use and development of the technology. The *Partnership* includes experts in information technology, patient safety, human

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

factors, systems implementation, and healthcare operations, as well as the Expert Advisory Panel. Health IT system vendors serve as analytic contractors under the Patient Safety and Quality Improvement Act (PSQIA) and will help to analyze the data gathered by the *Partnership*.

3. **Leveraged learning**. The knowledge gained through the *Partnership* will be translated into meaningful practices, resources, and tools. Collaborating organizations will broadly disseminate these learnings via publications, at meetings, and through various professional organizations, many of which are participants in the *Partnership* and were present at Partnering for Success.

INFORMING THE NATIONAL STRATEGY FOR HEALTH IT PATIENT SAFETY

The *Partnership for Health IT Patient Safety* is applying and building on patient safety principles set forth by the Institute of Medicine (IOM), the Office of the National Coordinator for Health Information Technology (ONC), the Bipartisan Policy Center (BPC), and others to establish a meaningful national framework for health IT safety.

In the 2000 report *To Err Is Human: Building a Safer Health System*, IOM identified a national agenda for change, specifying actions that entities should take to improve patient safety, including the implementation of nonpunitive systems for reporting and analyzing errors. In 2012, IOM issued the report *Health IT and Patient Safety: Building Safer Systems for Better Care*, which stated that "to protect America's health, health IT must be designed and used in ways that maximize patient safety while minimizing harm." The report emphasizes that the improvement of health IT safety is a shared responsibility, especially since health IT products are part of a larger sociotechnical system that includes people, organizations, processes, and the external environment. "Safety emerges from the interaction among [these] factors," says IOM. The report underscores the importance of generating, developing, and sharing safety risks and recommends that reports by users be voluntary and that identities of reporters not be discoverable under any circumstance. "User-reported health IT–related adverse events should be collected by a central repository and also be sent to the appropriate vendor," says IOM.

The report from ONC published on July 2, 2013, *Health Information Technology Patient Safety Action & Surveillance Plan*, names two "fundamental objectives": first, to use health IT to improve the safety of patient care, and second, to constantly improve the safety of health IT use. "Achieving these objectives is a shared responsibility," states the report. The plan offers guidance for clinicians, nonclinical staff, patients and caregivers, the government, health IT developers, patient safety organizations (PSOs), accrediting bodies, and more. (ONC "Health . . . Patient Safety")

Likewise, the BPC report *An Oversight Framework for Assuring Patient Safety in Health Information Technology* identifies a set of principles that should guide strategic planning regarding health IT. These points include recognizing the role of health IT in improving patient care; ensuring that patient safety is a goal shared across the "entire health care system"; understanding that a health IT patient safety framework should be risk-based, flexible, and innovative; and underscoring the importance of reporting health IT-related patient safety issues. (BPC)

In 2014, *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* was published. This report recommended "the creation of an environment of learning and continual improvement," both to protect patient safety and foster innovation in health IT use. The FDASIA report recommended that such a learning environment should

1. Identify, report and respond to health IT-related adverse events and near misses;
2. Aggregate and analyze events and near misses to identify patterns and trends;
3. Share information about methodology, practices, policies, and findings in a transparent manner;
4. Support the development and adoption of interventions and mitigations, where appropriate; and
5. Promote system-wide education and learning for stakeholders resulting in a system that is continually undergoing improvement. (U.S. FDA et al.)

The IOM, ONC, FDASIA, and BPC reports all recognize a role for PSOs in gathering adverse event information in a nonpunitive environment under the privilege and confidentiality protections of the PSQIA. The Agency for Healthcare Research and Quality (AHRQ), the federal agency responsible for regulating PSOs and implementing the PSQIA, has published guidance for health IT developers that wish to work to improve patient safety within the framework of the Patient Safety and Quality Improvement Act of 2005. (AHRQ "Frequently")

"We're seeing a host of problems with health IT, and there are some big opportunities to make those things better," said David W. Bates, MD, MSc.

Is collaborative learning effective? Sharing the transportation industry's experience, speaker David Mayer, PhD, emphasized that a multi-stakeholder group can be an effective vehicle to improve the system as a whole without punitive action. "We investigate transportation disasters using [this] really unique nonadversarial collaborative process," he said. Called the Civil Aviation Safety Team (CAST), the group, much like the *Partnership*, involves multiple aviation stakeholders—ranging from airplane and engine manufacturers to pilots and flight attendants, as well as trade associations and federal regulators—addressing common safety concerns and identifying feasible solutions for all. "The participants in CAST made a conscious decision not to compete on safety," he explained. "You're embarking on a collaboration that's really similar to this, and that's why I'm really excited about what you're doing," he told *Partnership* participants.

Identification of Health IT Safety Issues

Bates outlined the risks and benefits of health IT use. "Overall, the literature suggests that health information technology clearly appears to improve safety," said Bates. "But, the literature also provides many stories that describe how health IT creates new safety risks. And I would submit that the magnitude of harm and the impact of health IT on patient safety is uncertain; that's because of the heterogeneous nature of health IT. We have very diverse clinical environments, workflows [that are] different from place to place. The evidence in the literature is still relatively limited."

Reports in the literature conflict regarding the efficacy of health IT implementation, said Bates. He cited one study that found an increase in mortality rates after a commercial computerized provider order entry (CPOE) system was introduced (Han et al.) but noted that other organizations later "introduced exactly the same commercial CPOE application [and] actually saw their mortality rates fall." Bates posited that the difference between CPOE implementation success and failure in these scenarios was "related to the way that the application was introduced." One participant noted that effective team support in implementation and problem resolution has advanced the effective use of the technology and changed the focus to a resolution of more specific issues related to the components of the technology. See the discussion Health IT Safety Identification, Triage, and Investigation, later in these Proceedings, for more information.

Other significant risks created by health IT are in the areas of interoperability (e.g., incorrect merging of data), use (e.g., medication selection and patient identification errors), and hardware/software issues (e.g., unexpected downtime, truncated displays, problematic default settings). Each of these areas was addressed specifically by groups of participants in breakout sessions, which are documented later in these Proceedings.

"It's quite clear that health IT can introduce new errors," said Bates. "We have to have better frameworks to describe them." This effort will require new definitions and classification systems, he explained. Likewise, he recommended that organizations develop approaches to identify, track, and engineer errors out of their systems.

Compounding the risk is the fact that organizations have no central data repository to which to report safety issues. "They generally don't get aggregated at the national level," explained Bates. And, he added, patient safety surveillance relies on self-reporting of adverse events, near misses, and hazardous conditions. Because such issues are self-reported, it can be complex to discern if health IT is a factor when analyzing reported events, especially if the event is not designated as such by the reporting organization or individual. If the reporting organization is not attuned to the IT component of voluntarily reported issues, it may not identify significant, relevant health IT-related information

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

when reporting the event for analysis.

Agreement on what precisely constitutes a health IT issue is a necessary foundational step. The challenges in determining what should be considered as a health IT-related event were illustrated in Bates' presentation, which included various case studies of potential health IT-related events. Bates presented several cases that involved health IT to a varying degree, seeking stakeholder perspectives on whether, in their judgment, the case would be considered a health IT safety issue and whether it would be reported as such within their organization and to the *Partnership*. Specifically, after each case was described, meeting participants were asked to anonymously indicate whether the issue involved was a health IT-related issue and if it should be reported. As shown in the following cases, participants were not always in agreement about whether the example simply involved health IT or was a health IT-related issue. In addition, there were varying opinions regarding who should handle the issue, demonstrating that even for those in the thick of health IT decision making, opinions can differ.

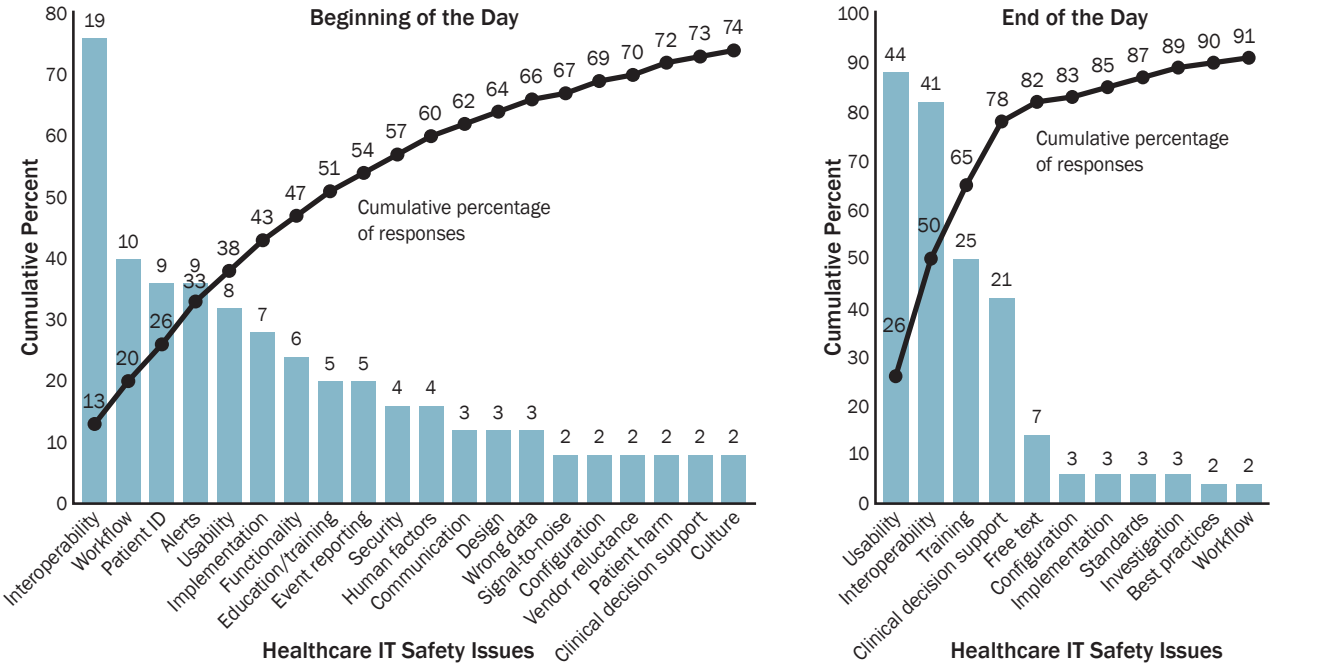
When determining what the current pressing concerns are, participants, through the use of anonymous polling, identified a vast array of differing issues. Throughout the course of the meeting, however, participants seemed to come to agreement regarding potential health IT priorities. See "Figure 1. Consensus on Important Health IT Safety Issues."

CASE 1: FREE-TEXT FIELD USED FOR LAB AND MEDICATION ORDERS

Facts: The provider documented care in the free-text fields of the electronic health record (EHR) system, including a medication order and lab order.

Background: The risks in such circumstances are that the orders will not be carried out or will not be carried out in a timely fashion, and that information will not be readily communicated to other providers or trigger the appropriate alerts and fail-safes designed to make care safer. Currently, most EHR systems are not able to read free-text fields and populate data according to information contained in those fields. Yet many providers are familiar with documentation by free text;

Figure 1. Consensus on Important Health IT Safety Issues

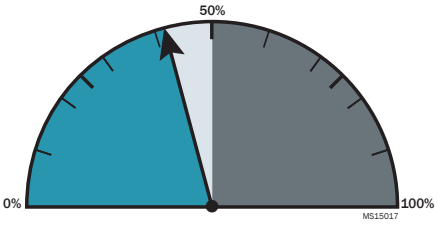


Participants in the Partnering for Success meeting were polled on the importance and priority of health IT safety issues during the day; as the meeting progressed, views changed. (Items with a count of 1 were omitted from the Pareto chart.)

MS15006

changing those practices (using the technology appropriately) may create patient safety vulnerabilities until there is adequate recognition of the capabilities and limitations of the technology.

Polling: When asked if this was a health IT issue, only 42% of participants agreed that it was. Half of participants believed it was not, while 8% were uncertain.

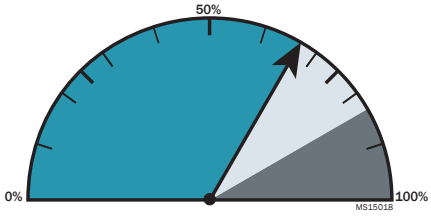


CASE 2: INCORRECT DATA ENTRY AND DROP-DOWN SELECTION

Facts: In another case, the provider began to type information into a data entry field, which brought the provider to a specific location in the field's drop-down menu. The provider had to choose the correct piece of information within the drop-down menu, but incorrect information was entered.

Background: Errors and unsafe conditions related to auto-population or auto-selection of data and drop-down menus can be a health IT risk. This type of error may be due to multiple factors. In some instances, selections are highlighted and automatically entered unless a provider chooses an item further down in the list. Additionally, "smart" applications recognize standard terms and auto-complete words or phrases with minimal prompting.

Polling: A majority of respondents, nearly 67%, indicated their belief that this was a health IT-related issue, while the rest of respondents were almost evenly divided between being uncertain and believing it was not health IT-related.

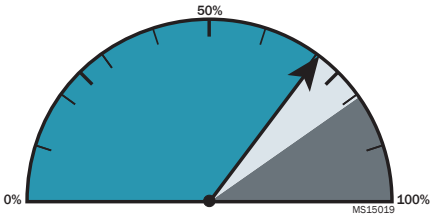


CASE 3: LACK OF SELECTIVITY AND SILENCED ALERTS

Facts: In a third case, a healthcare organization elected to turn off all red-flag (soft) alerts in their EHR system because the software did not allow alert selectivity. During one patient's short-stay procedure, Toradol was ordered, but the patient had an allergy to naproxen (an ibuprofen compound, an allergy to which contraindicates the prescription of Toradol) and experienced a reaction.

Background: Alerts in health IT systems are a complex and often under-considered source of risk. The creation of too many informational alerts can lead to the phenomenon known as alert fatigue, and the creation of either too many or too few alerts can lead to medication errors, order duplication, and other patient safety risks. When implemented deliberately and mindfully, alerts can be beneficial to patient safety and care quality. (ECRI Institute "Implementing") There is currently no standard regarding alert settings; to date, alarm setting decisions are made by individual facilities.

Polling: A majority of participants, 71%, agreed regarding this case, determining the issue to be health IT-related. Of the rest, 19% believed it not to be health IT-related, and 10% were uncertain.



The *Partnership* hopes to identify areas where alerts would be beneficial, work with software vendors to facilitate use, and determine best practices. This was one area recommended for deeper consideration as a result of participants' discussions during the meeting. (For more, see the discussion Immediate Advancement of Health IT Safety, later in these Proceedings.

THE IMPORTANCE OF REPORTING

Another barrier to learning is inadequate reporting. One participant, representing a healthcare organization, shared that her organization was often challenged to convince staff to report health IT safety issues, finding that they were reluctant to report issues for fear that vocalizing an issue meant that they would appear to not be using the technology appropriately or safely. In order to overcome this barrier, the participant highlighted the need to encourage reporting by reminding staff that "it's OK, and we're learning from this."

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

The *Partnership*'s learnings arise from the collection of a vast array of data, information, and stories. It was reinforced throughout the day that each contribution and interaction is important to collaborative learning and, ultimately, advancement.

Barriers to Building a Health IT Learning System

"If you . . . were to take a look at the Institute of Medicine report on this issue . . . , the work of the FDASIA workgroup . . . , the Bipartisan Policy Center report, and all of the other thought leadership pieces out there, you'd see the common theme around this whole issue is about building a learning healthcare system," explained moderator Janet Marchibroda, MBA.

"It really is a whole system that needs to work together," commented one participant.

Another stressed the importance of identifying and addressing barriers early "because [they] can really slow down [the] process" if they are discovered later.

As discussed by Dean Sittig, PhD, and Hardeep Singh, MD, MPH, during the meeting, key barriers to creating a learning system are the absence of widely accepted and useful taxonomies to describe health IT safety concerns and surrounding data and currently underdeveloped mechanisms of effectively reporting, aggregating, and analyzing data.

These concerns resonated with participants. One asked, "How [do we] collect the data in a standardized fashion so we can actually all use the data?" This participant worried that the combination of aging technology and a need to report desensitized or deidentified data would seem complex to practitioners. "I think that's a big barrier for us to overcome," said this participant.

Another participant pointed to the internal barriers to achieving learning for vendors, stating that while "no one wants to create software that has the potential to harm," getting IT professionals to "walk in a physician's shoes" is a challenge.

Limited understanding of clinical staff about health IT issues was also a barrier for another stakeholder, who found difficulties getting staff to recognize health IT issues. In order to overcome this barrier and align a common interpretation of events with health IT issues, one healthcare organization used broad-reaching policies to help prevent unintended consequences of health IT use. These policies included definitions of IT staff member and health IT senior staff roles, a procedure for reporting IT systems issues, a list of information required in a health IT safety report and steps for reporting, a flowchart of the path each issue would take during analysis, and an assessment of the degree of issue criticality and the response required. (Veterans Health Administration/Office of Information)

A participant representing a professional society believes that another barrier to the learning system that the *Partnership* will need to address is identifying health IT solutions that are "simple and elegant" in order to receive buy-in from the healthcare world and that the group must determine which high-priority health IT issues to tackle.

Developing a Common Language for Health IT Safety Issues

"Measurement is the first step to improvement," said Singh. Speaking about the importance of identifying a standard scheme for classifying health IT-related safety concerns, he noted, "It's very clear that a lot of us are not on the same page." By sharing a common language for classifying events, *Partnership* stakeholders can more easily measure and assess the shared data and share lessons to improve health IT.

The *Partnership* uses two standardized approaches to help providers uniformly report patient safety events and hazards: (1) AHRQ's Common Formats for reporting health IT issues and unsafe conditions and (2) Hazard Manager, a management tool and ontology that captures information about health IT hazards before they can cause harm. Hazard Manager was developed with funding from AHRQ. (AHRQ "Health Information") The *Partnership* may identify opportunities to improve upon these taxonomies in order to collect actionable information to clarify parameters of focus. For more information about these standardized taxonomies, see "Standardized Taxonomies for Health IT Issues."

The use of a common vocabulary and proper classification of a health IT issue or event can help to enhance an organization's response to an event, hazardous condition, or near miss. (ONC "Health . . . Adverse")

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Said one *Partnership* participant: "How you classify [an event] will be how you manage it."

Simply knowing that technology was involved allows organizations to better realize the potential risks and safeguards inherent in its use. Sittig proposed five types of health IT-related safety concerns that should be considered when evaluating health IT issues. He described them as follows:

1. The health IT system fails. In these instances, the system either fails during use or is otherwise not working as designed. For example, Sittig recalled a case of a patient who was taking 100 mg of a medication. Because the facility where he was hospitalized stocked only 25 mg pills of the medication, the patient was prescribed four of the 25 mg pills at a time. At discharge, the system merged the outpatient dose of 100 mg and the quantity of pills from the inpatient encounter and indicated that the patient should receive 400 mg of the medication. "It turned out that the problem had happened to 50 other patients, but no one had caught the mistake." These instances of hardware or software not working "need to be talked about, and they need to be fixed as soon as possible," said Sittig.
2. The health IT system works as designed but does not meet the user's expectations. In these situations, there's a mismatch in how the system is designed and how it is used. "Usually we talk about these as usability issues," he said. "That's when we really need to work together" with the vendor. "The developers have a mental model about how it should work, and the users have a [different] mental model."
3. The health IT system is working as designed but is not configured correctly. A good example, said Sittig, is duplicate alerts for pain medication to be taken on an as-needed basis (e.g., when two pain medications are prescribed—one short-acting and one long-acting). In these situations, the computer may look at a duplicate order for pain medication and give a duplicate warning, even though the medication is prescribed as needed. "It's working as designed, but it's really not what we tried to configure."
4. The health IT system is working as designed and configured,

STANDARDIZED TAXONOMIES FOR HEALTH IT ISSUES

By using a common language for identifying and reporting health IT-related safety concerns, organizations are better positioned for leveraged learning. Not only can they share their health IT event data, but they can also benefit from any lessons learned from the aggregated data. The *Partnership* is currently using two formats for identifying health IT issues.

AHRQ Common Formats. AHRQ's Common Formats use common definitions and reporting formats for PSOs to collect information from providers and standardize how patient safety events are represented. The most recent version of the Common Formats (version 1.2) includes an event report for health IT issues and unsafe conditions, enabling providers to report these events in a systematic manner and allowing PSOs to aggregate the data.

AHRQ's health IT event report asks up to six questions about the event or unsafe condition. For example, the report asks the organization to characterize the health IT product involved in the event as one of the following: administrative/billing or practice management system; automated dispensing system; EHR or EHR component; human interface device (e.g., keyboard mouse, touchscreen, speech recognition system, monitor/display, printer); laboratory information system, including microbiology and pathology systems; radiology/diagnostic imaging system, including picture archiving and communications systems; or other (and described by the event reporter).

Hazard Manager. Hazard Manager is a management tool and ontology that provides a common language for systematically reporting health IT events and hazards. The reporting tool provides formats for important event report parameters such as the event description, health IT systems involved, discovery of the event, causes of the event (e.g., usability, data quality, decision support), and impact of the event on care processes.

The *Partnership* obtains information about the specific vendor, system, version, and module for each IT system being used in provider facilities. Each system is often unique in how it functions and interfaces with other systems; learning how these systems interface and identifying commonalities among events can improve overall safety.

See "Appendix A: Hazard Manager Taxonomy" for more information on the Hazard Manager taxonomy.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

but an interaction with another system causes problems. As an example, Sittig described an unintended interaction between a health IT system and an admission, discharge, and transfer (ADT) system. Anytime the patient was transferred, the ADT system discontinued the patient's medications and required the user to reenter the patient's medications. Even when a patient was transferred from one bed to another, the ADT system still classified the encounter as requiring that the patient's medications be discontinued and reentered for the new setting. "It's very difficult to test for this [how different IT systems interact] because you can't imagine how everyone is going to connect all these systems together," said Sittig.

5. Specific health IT safety features or functions were not implemented or were unavailable. In some instances, an event occurs that could have been prevented with a particular health IT system feature. For example, say a hospitalized patient inadvertently receives more than the recommended maximum daily dose of a medication; an alert could stop this from happening. Said Sittig, "These are things we want to have happen. This is the goal of health IT."

Reporting Health IT Issues to the *Partnership*

Because of uncertainty about the unsafe conditions and risks associated with health IT, the *Partnership for Health IT Patient Safety* is collecting a variety of reports about health IT-related safety issues to inform the national safety strategy for health IT and to determine which issues on which to focus its efforts. *Partnership* stakeholders agree that health IT provides numerous benefits, such as supporting clinical decision making, enhancing provider communication, providing access to patient data in a secure environment, engaging patients, and reducing medical errors.

Participants recognize, however, that health IT can create new safety risks if it is not designed appropriately, implemented carefully, and used thoughtfully (ECRI Institute "ECRI Institute PSO Deep Dive"; Sparnon and Marella). Analyzing data about health IT-related safety concerns collected by all the *Partnership* stakeholders can provide insights into identifying factors that contribute to these concerns and developing strategies to prevent similar problems from arising.

At the meeting, participants sought to identify the types of reports addressing health IT-related safety concerns that should be shared among *Partnership* stakeholders for leveraged learning. They also considered the format for submitting some of the reports in order to collect the necessary information about a particular health IT-related issue.

REPORT TYPES TO SHARE

Solomon identified the multiple sources of data for health IT-related safety concerns collected by the *Partnership*: adverse event reports, near misses, help desk tickets, system alerts, root-cause analyses, and more. The data is analyzed to identify factors that contribute to the problem and to distill any lessons to improve health IT safety and to share with health IT stakeholders.

Event reports of health IT-related issues collected by healthcare facilities and health IT vendors are valuable sources of data for improving health IT safety, but they are not the only source for information. The *Partnership* is collecting data from multiple sources, including the following:

- Adverse event and near-miss reports from healthcare organizations
- Help desk requests submitted by healthcare facility staff to their IT departments and their health IT vendor
- Alerts from vendors sent to their health IT system users
- Vendor summary data
- Assessment data
- Root-cause analyses and investigations of health IT-related safety concerns and events conducted by healthcare facilities and vendors
- Published evidence-based research
- Reports of health IT-related events submitted to the U.S. Food and Drug Administration's medical device reporting programs (e.g., Manufacturer and User Facility Device Experience database, MedSun)

One participant noted that medical professional liability claims data can also be an important information source, as has been the case with understanding the factors affecting diagnostic errors and obstetric safety. Through collaborating organizations, the *Partnership* anticipates adding this type of information to its analysis. Given that there is sometimes a delay before a claim is filed following an alleged event, claims related to health IT issues may take time to emerge as the technology gains widespread use.

This participant reiterated that some malpractice claims related to health IT may not be clearly identified as such by the reporting organization. "We tend to think there's a lot more under the radar that we're not even identifying," the participant commented.

HEALTH IT ISSUES THAT WARRANT REPORTING

Health IT reporting programs, such as the *Partnership*'s reporting initiative, should identify a list of serious safety concerns associated with health IT that must always be reported, recommended Sittig. He gave meeting participants an advance look at a list of eight "must report" health IT safety events that he and coauthor Singh have proposed if a federal center is established to monitor health IT safety. (Sittig et al.) There is no consensus yet on mandating the reporting of certain issues, and valuable learning is often obtained from reports regarding the unanticipated issues.

Regarding these eight health IT safety issues, Sittig said, "These are serious events. Every time they happen, they should be reported." As an example, he listed computerized alerts with high clinician override rates. When an alert is always overridden, "that's saying something is wrong. It's not working," so it should be reported, he said.

The eight suggested reportable health IT safety issues are as follows (Sittig et al.):

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

This list of must-report health IT events has been proposed for national efforts to monitor health IT safety. Individual healthcare facilities may want to collect types of problems and near misses that exceed the list's scope. For example, while a national program may be interested in limiting reports of software errors to those affecting multiple patients, individual healthcare facilities may want to collect reports of any software calculation error.

REPORTING NEAR MISSES: IMPROVEMENT PRIOR TO HARM

Partnership stakeholders did not want to limit reporting only to events that cause patient harm. They supported the need for reporting and analyzing all types of incidents, including those that do not cause any harm, near-miss incidents, and circumstances that precede an actual event and are caught before anything can happen (i.e., hazardous conditions). Likewise, participants are interested in contributing information about instances in which technology has been used to make care safer. In order to properly analyze all such information and identify best practices, "It will be useful to collect lots of [events] and to use techniques like natural language processing and other approaches to go through them rapidly and classify them in various ways," said Bates.

In fact, many of the event reports submitted to ECRI Institute PSO are near-miss events. Analyzing these reports provides "an opportunity to make improvement" before patients are harmed, said Solomon. "They may not have actually caused harm, but they have the opportunity to cause harm." In addition, the *Partnership* is examining help desk logs; these can help to identify potential issues before they affect patient safety.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

REPORTING FROM ALL PHASES OF THE HEALTH IT LIFE CYCLE

Reporting of health IT events, issues, and hazards should cover all phases of the technology's life cycle, said Singh. Each phase of the life cycle represents a step in the technology's evolution; consequently, different types of events may arise during each of the three phases and should be captured in the *Partnership*'s collection and analysis of health IT-related issues.

There are three phases to health IT; each phase can affect patient safety differently, said Singh. As a result, organizations must heed the incidents arising during each phase to ensure health IT safety. The phases are as follows (Sittig and Singh "Electronic Health Records"):

Phase One: Safe IT implementation. During the early stages of health IT's life cycle, the focus is on implementing the technology and ensuring its safe use. Events during this first stage typically involve implementation issues. Are the system interfaces fully functional? Is the software configured to accomplish tasks as expected? As an example of a phase one event, a computer glitch in a medication ordering system mistakenly prescribed a male impotence drug for 900 smokers seeking an antismoking medication; the electronic formulary selected a list of the most popular medications, and the wrong medication was inadvertently selected.

Phase Two: Using IT safely. As the healthcare staff adjust to use health IT, phase two dominates. Events during this stage involve the unsafe or inappropriate use of the technology by people and their organizations. For example, has the organization set up too many computerized alerts, leading clinicians to overlook critical alerts because of information overload? This is a "classic example" of a phase two problem, said Singh. In one study, prescribers reported receiving a median of 63 alerts per day; nearly 87% of respondents perceived this to be excessive, nearly 70% believed they could not effectively manage these alerts, nearly 55% reported the potential for test results to be missed, and nearly 30% reported having missed a result that led to a delay in care because of the excessive alerts (Singh et al.).

Phase Three: Using IT to monitor and improve safety. At this stage, health IT reaches its intended goal to improve and monitor safety. Events during phase three are triggered when the system detects medical errors and gaps in patient care, such as identifying patients who have not received follow-up for abnormal cancer screening tests. "We're not all there yet because we're mostly struggling with phase one and phase two," said Singh. Another factor to consider: improvement and monitoring may be performed very differently and have different indicators and outcomes for individual organizations. The final goal of effective, improved patient care—rather than just meeting quality indicators without really doing the work—must always be kept foremost in mind. (See "Figure 2. Health IT Life Cycle" for more.)

REPORTING ACROSS THE CONTINUUM OF CARE

Partnership participants also recognized that reporting of health IT safety concerns should extend across the continuum of care and include events from hospitals, physician practices, long-term care facilities, and other settings connected to a health IT system. As the patient moves from one healthcare setting to another, the patient's data is likely entered into different health IT systems. Currently, the interoperability of these systems is imperfect, which can limit clinicians' understanding of the patient's continuity of care across the continuum. Participants in the day's meeting indicated that interoperability is one of their primary concerns regarding health IT safety.

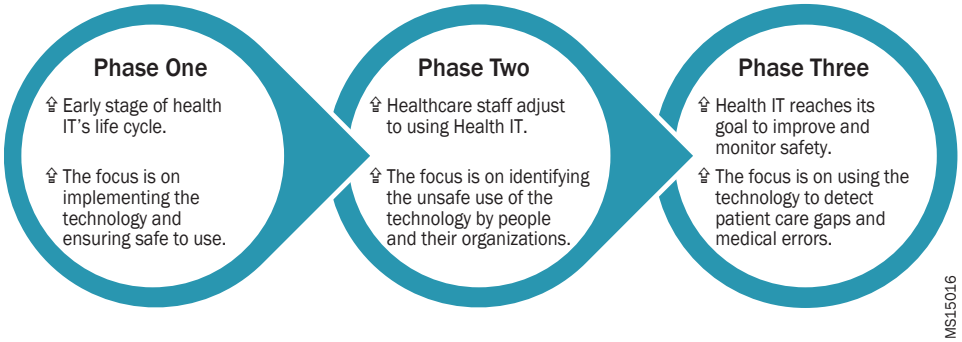
"We need to think about the longitudinal patient journey as patients receive care in different settings," said Singh. Reporting of health IT interoperability concerns across the continuum can provide insights into the safety issues. "We don't have the data because we're so dispersed with our IT systems and fragmented," he said.

Health IT Safety Identification, Triage, and Investigation

"What are the key characteristics of a successful health IT safety identification, triage, and investigation system?" asked Marchibroda. Participants considered the necessary components of a process for identifying, triaging,

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Figure 2. Health IT Life Cycle



Source: Sittig DF, Singh H. Electronic health records and national patient-safety goals. N Engl J Med 2012 Nov 8;367(19):1854-60.

and investigating health IT safety issues. Terhilda Garrido, MPH, ELP, of Kaiser Permanente, stressed the importance of working with health IT vendors and health IT stakeholders when identifying and managing health IT safety events.

"We absolutely need our health IT vendors to be working with organizations as we problem solve," Garrido emphasized to *Partnership* stakeholders. "Neither of us has the sole expertise or understanding in such a complex system of how to both identify and remediate these things." See "Kaiser Permanente's Systematic Approach to Solving Health IT Concerns" for a description of the healthcare system's approach.

Another health system noted that it retained a core group of its 180-person health IT implementation team to continue to meet weekly to review current issues from a quality and safety perspective. When the health IT system was phased in at the various hospitals, the team staffed a command center to monitor reports as they were coming in and tracked their resolution.

"There's a portion of the team that still exists . . . to look at the issues that are coming in [and address] how do we deal with those issues, what kind of changes do we need to make," noted the participant.

Throughout the meeting, participants identified various characteristics of an effective health IT safety reporting program, including the following:

- **Make reporting of health IT safety concerns easy** for users; otherwise, users are less likely to report problems they encounter even though they have been told that the information is needed to improve health IT safety. "We should be able to set this up so that reporting is really simple," recommended Bates.
- **Recognize the limitations** encountered by some settings in reporting health IT safety issues. Physician practices, for example, typically do not have an IT department for reporting their concerns. Instead, they will report the problems they encounter to the system vendor, said one meeting participant.
- **Establish a nonpunitive environment,** free of any finger-pointing, for reporting and identifying problems with health IT. As one meeting attendee said, "You bring everybody to the table, and everybody can contribute to solutions."
- **Adopt a multidimensional approach** to analyzing health IT-related events to understand the many factors that can contribute to health IT safety issues. One approach is to use the sociotechnical model developed by Sittig and Singh and described in "Sociotechnical Model for Health IT Event Investigation."

Immediate Advancement of Health IT Safety

When asked by an audience member about how the *Partnership* members can break down barriers and keep stakeholders engaged, one panel member used an appropriate analogy: "How do you eat an elephant? Piece by piece."

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

KAISER PERMANENTE'S SYSTEMATIC APPROACH TO SOLVING HEALTH IT CONCERNS

Garrido, Kaiser Permanente's vice president of health IT transformation and analytics in national quality, gave participants a peek behind the curtain at Kaiser Permanente's HealthConnect system, which has been in place for nearly 10 years and bridges its three core operations: the health plan (serving 9.5 million lives), a system of 37 hospitals, and a network of 17,000 physicians.

Triage. Users report health IT problems and concerns to an IT help desk, where a representative decides whether the concern can be easily addressed (e.g., "How do I get my printer working?") or needs to be triaged for further evaluation.

Collaboration and follow-up. Once the issue is triaged for further evaluation, Kaiser Permanente follows a four-step process called PART (i.e., prepare, assess, remediate, and track), which may engage multiple stakeholders, such as frontline physicians, providers, and staff; Kaiser Permanente's IT and HealthConnect staff; patient safety experts; medical informatics leaders; and others.

The team assigned to the particular safety issue identifies the nature of the concern and its impact on patient safety. For example, Garrido asked, is it related to software coding, workflow, system configuration, or user training? Coding problems are reported to the vendor, thus bringing the vendor into the investigation. Separately, the vendor will also bring safety issues to the health plan's attention when they are identified by the vendor's own internal assessments and feedback from its customers.

Garrido noted that the types of health IT concerns currently addressed by Kaiser Permanente "are very different from the issues we identified in the past. Our processes have improved." Previously, many of the issues were identified by HealthConnect users; now, the majority of health IT-related issues are raised by the vendor, which communicates regularly with the health plan about software coding changes and updates.

Additionally, the number of health IT safety concerns raised by system users has decreased as more become experienced with its health IT system. The team responding to health IT safety concerns has settled into "a rhythm" and an "understanding of what are the right paths to take to remediate issues," said Garrido.

Once the concern is remediated, the issues continue to be tracked to determine if the mitigation strategy is successful and feedback is provided on an intranet site to those involved.

Using data to improve. As a measure of success, Garrido said the number of professional liability claims per 100,000 members has declined since the system was adopted. Additionally, Kaiser Permanente has been able to use the patient data stored in HealthConnect to improve quality of care provided to its health plan members by identifying, for example, those plan members who have not received necessary immunizations and cancer screening procedures and reminding them of these important prevention measures.

Recounting a personal anecdote about a physician who was so excited about his new EHR system that he couldn't stop talking about it at a party, this participant posited that working individually with champions at different healthcare organizations will help to ensure buy-in and success in making health IT safer for patients.

Another panel member commented that while there are issues with health IT that need to be addressed, it has had a positive effect on many different aspects of healthcare. One way this participant's organization has been able to foster innovation and bring new ideas to the table is by offering member facilities monetary "risk reduction awards" through a contest wherein individuals submit proposals for patient safety improvements; almost two-thirds of the submissions for the first set of awards were related to health IT.

To facilitate and encourage reporting, *Partnership* participants were given two tools to promote health IT safety at their organizations: a "thank you" card to give out to staff who submit reports and a flyer to inform other stakeholders of the *Partnership*. Another resource for organizations to help identify issues with health IT that was mentioned frequently were the nine ONC's SAFER guides, which are available at http://www.healthit.gov/safer/safer-guides.

At the meeting, participants worked together in breakout sessions to share and recommend potential strategies that can help to strengthen health IT safety and usage. These groups focused on use and user error, interoperability issues, and hardware/software issues. The goals of the breakout sessions were to identify the characteristics of each of the three focus topics, to create discussion questions to help in the identification of the issues, to determine the best way to report the issue, to identify follow-up actions based on stakeholder experience, and

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

to determine how learning from the actions taken can be disseminated.

The use and user error breakout groups sought to define the line between an error due to the technology and an error made by the user when using the technology (e.g., entering incorrect data). Here, training and user accountability are key. Additionally, understanding which systems should be standardized and which systems are best left to be configured by the individual organization is also important. These groups discussed the ways in which system design or appearance can help or hinder system use. The goal, agreed breakout session participants, is for the system to make the correct action be the easiest one to take.

The interoperability breakout groups debated how to identify interoperability issues, methods of reporting interoperability issues, and to whom such issues should be reported. Here, ensuring that data is timely and reliable and that access is possible across the continuum is vitally important. Concern that errors can be easily multiplied as systems share and communicate information in different platforms is a challenge, as data needs to be accessed in a multitude of systems. Participants agreed, however, that reporting such issues should be simple for practitioners because the ease of reporting increases the likelihood that issues will be reported and errors will be corrected early.

The hardware/software groups agreed that the identification of health IT safety issues is complex and difficult and that issues go underreported. System downtimes are a challenge. Processes need to be in place to accommodate care and obtain information about patients during what could be an extended period of outage. Moreover, providers are challenged in populating that information back into the record once a system is again operable. Understanding the system vulnerabilities is important. Thus, the groups discussed the value of simulation testing before systems are implemented, as well as that of testing systems after each upgrade. The importance of evaluating hardware and software installations from a high-reliability perspective was also discussed.

Each breakout group suggested several strategies to combat identified health IT safety issues. See "Potential Health IT Improvement Strategies" for strategies that were identified as a result of these breakout sessions.

SOCIOTECHNICAL MODEL FOR HEALTH IT EVENT INVESTIGATION

Sittig and Singh have coined the concept of the sociotechnical model for investigating health IT issues in healthcare settings. The model recognizes that health IT does not operate in isolation and must be evaluated within the context of eight dimensions that affect a health IT system's function.

"In our work, we go through every dimension in almost every case to figure out what exactly went wrong," said Singh. With most health IT events, "more than one dimension is involved."

The eight dimensions of the model are as follows:

1. Hardware and software (e.g., computers, keyboards, data storage, software to run health IT applications)
2. Content (data, information, and knowledge stored in the system)
3. User interface (hardware and software interfaces that allow users to interact with the system)
4. Personnel (software developers, IT department personnel, clinicians, healthcare staff, patients, and others involved in health IT development, implementation, and use)
5. Workflow and communication (steps followed to ensure patients receive the care they need at the time they need it)
6. Organizational policies, procedures, and culture (internal organizational factors, such as capital budgets, IT policies, and event reporting systems, which affect all aspects of health IT development, implementation, use, and monitoring)
7. External rules and regulations (external forces, such as federal and state rules to ensure privacy and security protections and federal payment incentives to spur health IT adoption)
8. Measurement and monitoring (processes to measure and monitor health IT features and functions)

Source: Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care* 2010 Oct;19 Suppl 3:i68-74. Also available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3120130 PubMed: http://www.ncbi.nlm.nih.gov/pubmed/20959322

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Disseminating Tools and Best Practices

Sharing information, including tools and best practices, was a common theme at the Partnering for Success meeting. Many of the representatives of healthcare organizations were interested in what others were doing to combat issues such as aligning the inpatient and outpatient EHR systems and determining how best to use heath IT system alerts and alarms, as evidenced by discussion among the participants. At the beginning of the day, Solomon remarked that ECRI Institute has been involved in reporting for 40 years and has provided a collaborative for sharing and learning, so ECRI Institute understands that "if it's not a nonpunitive [reporting system], you don't get much data." (See "Appendix B: ECRI Institute Health IT Safety Resources" for additional information and tools.)

"How can organizations avoid these [health IT] issues?" asked Bates. "Well, there are some best practices, like in the IOM report, like in the SAFER guidelines, but they are not used pervasively today. And it's been hard to learn from the experiences of others. There's some sharing within users of individual vendors, and the vendors have been good about sharing stories, but that's uneven, and across vendors, we haven't done so well. So one of the things we need to do . . . is we need to identify some best practices and then spread them."

Tejal Gandhi, MD, MPH, CPPS, led a panel discussion on how the *Partnership* can build a health IT learning system and how organizations can create and share health IT safety information.

One participant uses e-mail, learning days, and symposiums to disseminate information among the healthcare facilities within the organization, but the most successful strategy that has been used is to convene groups with shared interests (e.g., obstetric safety) to improve care. The participant also discussed the importance of assembling various executives from each medical center to make up the patient safety committee, thereby supporting buy-in from each of the executive's facilities.

An IT vendor noted that its goal is to prevent health IT issues before they occur, and the major undertaking is to get IT workers on the vendor side to look at and test software as users would. In order to accomplish this, the organization shares customer stories, "even if they're painful," and other information in order to help staff understand what it's like for healthcare workers to use the system and the importance of changes to the system.

POTENTIAL HEALTH IT IMPROVEMENT STRATEGIES

- Establish a common vocabulary that defines health IT-related issues.
- Identify sources for information about health IT-related issues, such as event and near-miss reports, help desk requests, user alerts, and root-cause analyses.
- Create awareness among health IT users to recognize and report health IT-related issues.
- Simplify the process for users to report health IT-related issues.
- Use a multidimensional approach to evaluating health IT-related issues to understand the many factors that can contribute to the problem (e.g., hardware and software, workflow and communication, organizational policies and procedures).
- Fully test a health IT system, including any upgrades and system improvements, for any unintended consequences before wide-scale adoption.
- Limit the number of medical records that can be opened concurrently.
- Limit copying and pasting of information from one record entry to another. Identify any information that is copied and pasted.
- Identify measures (e.g., percentage of clinical alert overrides, percentage of orders entered electronically) to monitor a health IT system's effectiveness.
- Provide comprehensive training to health IT system users; include information about what can go wrong so that users are aware of the system's possible unintended consequences.
- Ask vendors to provide guidance about any limits to configuring the health IT system to an organization's perceived needs.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

"There is a phenomenal appetite for this data," commented one participant. "We hear it all the time in our own organization. . . . So just even having that platform where we are publishing and [sharing] evidence-based information [is beneficial], because people are really groping in the dark right now for things. Everybody wants to know [if] someone else has tackled this and made some progress with it." This is a benefit of the *Partnership*; it is transparent, and issues and learning are shared among participants.

Participants believe that the *Partnership* will be useful in getting people to work together more effectively. For example, one participant recounted how the surgical departments at a healthcare organization were all experiencing a similar health IT issue and had the same vendor; yet in contacting the vendor, they each received different feedback on the issue and were approaching it differently. Knowing others were addressing the issue at the time would have been useful. "It was just a big 'aha' moment," said this participant; it led to a decision to approach the problem together in order to identify the best solution. Likewise, identifying shared problems and working on them centrally through the *Partnership* can lead to a more efficient and effective outcome.

Indeed, another participant noted that having such data available as a resource is valuable on its own. "It would help provide that evidence base for changing practices. . . . To be able to [use data from the *Partnership*] and have the ability to say 'it's not just us,'" would be invaluable, this participant explained, as would feeding back into the system to share the learnings.

Another participant hopes to use such information to educate and train staff. This vendor representative believes that the data will "give them the tools to understand how [the system] could be used or how the software could be used to the best of our ability to prevent [issues] from occurring." She further believes that the *Partnership* can be beneficial by eliminating the fear of reprisal that many vendors have about speaking out about health IT issues.

Hospital participants detailed the struggles they have implementing EHR and other health IT systems into their facilities. Participants agreed that criteria for health IT "must have" features and settings would be useful to help ensure that EHR implementation is performed safely. Participants felt that vendors likely know what is working and not working, but there's a discomfort in telling a hospital how to set up the system. One suggestion was voiced for an Amazon-like "suggestion" regarding how to set up EHR systems (e.g., if you are a 50-bed rural hospital, here is what most facilities like you have chosen to do).

Participants discussed the difficulty of reaching out blindly to other hospitals for suggestions on how to implement EHRs. One participant pointed out that "crowdsourcing" this information can be problematic because some outliers may actually be more advanced than most other facilities. But participants agreed that having a forum to discuss what issues occurred during implementation would be helpful to others.

For additional best practices, see "Kaiser Permanente's Systematic Approach to Solving Health IT Concerns."

Commitment to Goals and Follow-Up

The Partnering for Success meeting provided many points of discussion; however, Singh pressed the group for specifics: "What are three things we can think about over the next year?"

In response, many participants volunteered to form working groups to tackle the issues identified at the Partnering for Success meeting. Workgroups will study why the reported events occurred and identify best practices for preventing their recurrence. Topics being considered by the *Partnership*'s Expert Advisory Panel include the following:

- Auto-completion of text in critical data entry fields
- Copy-paste or cut-paste in progress notes
- Limiting the amount of records able to be opened simultaneously
- Determination of items available in drop-down lists and conformation of item selection
- Elimination of unacknowledged communication
- Use of Tall Man lettering (Institute for Safe Medication Practices)
- Elimination of "renew all" or "transfer all" functions
- Reduction of over-alerting

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

- Elimination of automatic end times for certain medication schedules
- Establishment of standard recent test result on-screen location
- Identification of methods to address wrong-patient chart entries
- Identification of staff training and training verification strategies for health IT systems

LOOKING FORWARD

One participant shared her excitement about the model for shared learning sought by *Partnership* stakeholders. "For us, this really does represent a different way of thinking and a different way of doing work together across the health IT stakeholder community," she said. "We're excited to be in the same room with providers, academics, professional organizations, and thought leaders. . . . We really look forward to doing things differently and working with this group."

"I think it truly is the innovation that we're all in the room together, working together," Solomon said to close the day. "This is the group that's going to make something happen."

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

References

Agency for Healthcare Research and Quality (AHRQ):

Frequently asked questions: health information technology (HIT) [online]. [cited 2015 Jan 9]. http://www.pso.ahrq.gov/faq#hit

Health information technology hazard manager (Pennsylvania) [online]. [cited 2015 Jan 9]. http://healthit.ahrq.gov/ahrq-funded-projects/health-information-technology-hazard-manager

Bipartisan Policy Center (BPC). An oversight framework for assuring patient safety in health information technology [online]. 2013 Feb 13 [cited 2015 Jan 9]. http://bipartisanpolicy.org/library/report/oversight-framework-assuring-patient-safety-health-information-technology

ECRI Institute:

ECRI Institute PSO Deep Dive: health information technology [online]. 2013 Mar 22 [cited 2015 Jan 9]. Available with subscription at https://www.ecri.org/components/PSOCore/Pages/DeepDive0113.aspx Available for purchase at https://eshop.ecri.org/p-140-pso-deep-dive-health-information-technology.aspx

Implementing computerized provider order entry [online]. Healthc Risk Control 2011 Jul [cited 2015 Jan 9]. Available with subscription at https://members2.ecri.org/Components/HRC/Pages/Pharm6.aspx

Han YY, Carcilla JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics* 2005 Dec;116(6):1506-12. Also available at http://pediatrics.aappublications.org/content/116/6/1506.long PubMed: http://www.ncbi.nlm.nih.gov/pubmed/16322178

Institute for Safe Medication Practices. FDA and ISMP lists of look-alike drug names with recommended tall man letters [online]. 2011 [cited 2015 Jan 9]. http://www.ismp.org/tools/tallmanletters.pdf

Institute of Medicine (IOM). Health IT and patient safety: building safer systems for better care [online]. 2011 Nov 8 [cited 2015 Jan 9]. http://www.iom.edu/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx

Office of the National Coordinator for Health Information Technology (ONC):

Health information technology adverse event reporting: analysis of two databases [online]. 2014 Nov 25 [cited 2015 Jan 9]. http://healthit.gov/sites/default/files/Health_IT_PSO_Analysis_Final_Report_11-25-14.pdf

Health information technology patient safety action & surveillance plan [online]. 2013 Jul 2 [cited 2015 Jan 9]. http://www.healthit.gov/sites/default/files/safety_plan_master.pdf

Singh H, Spitzmueller C, Petersen NJ, et al. Information overload and missed test results in electronic health record-based settings. *JAMA Intern Med* 2013 Apr 22;173(8):702-4. Also available at http://archinte.jamanetwork.com/article.aspx?articleid=1657753 PubMed: http://www.ncbi.nlm.nih.gov/pubmed/23460235

Sittig DF, Classen DC, Singh H. Patient safety goals for the proposed Federal Health Information Technology Safety Center. *J Am Med Inform Assoc* 2014 Oct 20; epub ahead of print. Also available at http://jamia.oxfordjournals.org/content/early/2014/11/07/amiajnl-2014-002988.long

Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care* 2010 Oct;19 Suppl 3:i68-74. Also available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3120130 PubMed: http://www.ncbi.nlm.nih.gov/pubmed/20959322

Sittig DF, Singh H. Electronic health records and national patient-safety goals. *N Engl J Med* 2012 Nov 8;367(19):1854-60. Also available at http://www.nejm.org/doi/full/10.1056/NEJMsb1205420 PubMed: http://www.ncbi.nlm.nih.gov/pubmed/23134389

Sparnon E, Marella WM. The role of the electronic health record in patient safety events. Pa Patient Saf Advis [online] 2012 Dec [cited 2015 Jan 9]. http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2012/Dec;9(4)/Pages/113.aspx

U.S. Food and Drug Administration (FDA), Federal Communications Commission, Office of the National Coordinator for Health Information Technology. FDASIA health IT report: proposed strategy and recommendations for a risk-based framework [online]. 2014 Apr [cited 2015 Jan 9]. http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf

Veterans Health Administration/Office of Information. 2004-2006. Used with permission.

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Appendix A: Hazard Manager Taxonomy Definitions

care process: A care delivery process involves any or all of the following: (1) problem recognition/assessment, (2) cause identification/diagnosis, (3) management/treatment, and (4) monitoring. Care processes typically involve more than one person (e.g., a physician prescribing a medication, a pharmacist dispensing the medication, and a nurse administering the medication to the patient).

compromised care process: Any care process abnormality that has the potential to contribute to patient harm.

end users: Clinicians (e.g., nurses, physicians, pharmacists), patients, or others who use health IT applications.

excessive nonspecific recommendations/alerts: A proportion of incorrect alerts (given a comprehensive understanding of the patient's situation) that is high enough to increase the likelihood of a clinician (1) making an error or (2) decreasing attention to future alerts.

health IT: Any electronic health information system, including electronic health records, health information exchange, or patient health records.

health IT hazard: Any characteristic of a health IT application or of its interactions with another healthcare system that increases the risk that care processes will be compromised and patients harmed.

mismatch between user mental models/expectations and HIT: Any difference between the way a user believes health IT should work and the way the health IT was designed to work.

situation awareness: A clinician's understanding of the patient's situation and how their actions and other events will affect the patient.

unusable software implementation tools: Tools provided by the health IT developer that make it hard for implementation teams to configure the system and manage subsequent changes to the system.

use error: Any use of health IT that increases the likelihood of patient harm.

value-added reseller: A company that adds features or services to an existing product, then resells it to a care delivery organization as a stand-alone product or part of an integrated solution. The added value can come from professional services such as integrating, customizing, consulting, training, or implementation.

Source: Agency for Healthcare Research and Quality. Health information technology hazard manager (Pennsylvania) [online]. [cited 2015 Jan 9]. http://healthit.ahrq.gov/ahrq-funded-projects/health-information-technology-hazard-manager

PARTNERSHIP *for* HEALTH IT PATIENT SAFETY
Making healthcare safer together

Appendix B: ECRI Institute Health IT Safety Resources

- Alarm Safety Resource Center.* https://www.ecri.org/alarm-safety
- ECRI Institute PSO Deep Dive: Health Information Technology.* https://eshop.ecri.org/p-140-pso-deep-dive-health-information-technology.aspx
- ECRI Institute PSO Deep Dive: Laboratory Events.* https://eshop.ecri.org/p-171-pso-deep-dive-laboratory-related-safety-events.aspx
- ECRI Institute PSO Deep Dive: Medication Safety.* https://eshop.ecri.org/p-142-pso-deep-dive-medication-safety-events.aspx
- Guidance article: Electronic Health Records. https://www.ecri.org/components/HRC/Pages/MedRec1_1.aspx
- Guidance article: Implementing Computerized Provider Order Entry. https://www.ecri.org/components/HRC/Pages/Pharm6.aspx
- Patient Safety at Intersection of Medical and Information Technology. https://www.ecri.org/components/PSOCore/Pages/PSONav0811.aspx
- Risk Managers' 10 Strategies for Health IT Success. https://www.ecri.org/components/HRC/Pages/RMRep0613_Focus.aspx
- Top 10 Health Technology Hazards for 2015.* https://www.ecri.org/Pages/2015-Hazards.aspx
- Top 10 Patient Safety Concerns for Healthcare Organizations.* 2014. https://www.ecri.org/components/HRC/Pages/RMRep0414_Focus.aspx

* These items are available without membership.

PARTNERSHIP *for*
HEALTH IT PATIENT SAFETY
Making healthcare safer together

Sponsored by
the Jayne Koskinas Ted Giovanis
Foundation for Health and Policy

ECRI Institute
The Discipline of Science. The Integrity of Independence.

For more information, contact hit@ecri.org