



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

Applying What We've Learned

Proceedings from the
October 16, 2015, meeting
convened by ECRI Institute

Sponsored by
 **JAYNE KOSKINAS
TED GIOVANIS** | Foundation for
Health and Policy

ECRIInstitute
The Discipline of Science. The Integrity of Independence.

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 M. Addis, MA, CPASRM
Risk Management Analyst

Paul A. Anderson
Director, Risk Management Publications

Jennifer Comerford, M.J., OTR/L, CHC
Risk Management Analyst;

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

Ellen S. Deutsch, MD, MS, FAAP, FACS, CPPS
Medical Director

Andrea Fenton
Web Editor

Jacqueline Ferenschak
Risk Management Analyst

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

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

Tara Kolb, Manager
Media Services

Ramya Krishnan, MS
Senior Project Engineer

William Marella, MBA
Executive Director, PSO Operations
and Analytics

Laurie Menyo, Director
Public Relations and Marketing
Communications

Jeremy Michel, MD, MHS
Physician Consultant, Technology Assessment

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

Amy Tsou, MD, MSc
Senior Research Analyst, Health Technology
Assessment, ECRI-Penn AHRQ Evidence
Based Practice Center (EPC)

Michael Wroblewski
Video Production/Design Specialist

Andrea Zavod
Managing Editor

Mission Statement

ECRI Institute, a nonprofit organization, dedicates itself to bringing the discipline of applied scientific research in healthcare to uncover the best approaches to improving patient care. As a pioneer in this science for nearly 50 years, ECRI Institute marries experience and independence with the objectivity of evidence-based research.

ECRI Institute, 5200 Butler Pike, Plymouth Meeting, PA 19462, USA; (610) 825-6000 (telephone); (610) 834-1275 (fax); info@ecri.org (e-mail).



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

Applying What We've Learned

Sponsored by
 **JAYNE KOSKINAS
TED GIOVANIS** | Foundation for
Health and Policy

ECRIInstitute
The Discipline of Science. The Integrity of Independence.



Acknowledgments

THE PARTNERSHIP FOR HEALTH IT PATIENT SAFETY EXPERT ADVISORY PANEL

David W. Bates, MD, MSc
Brigham and Women's Hospital

Pascale Carayon, PhD
University of Wisconsin-Madison College of Engineering

Tejal Gandhi, MD, MPH
National Patient Safety Foundation

Terhilda Garrido, MPH, ELP
Kaiser Permanente

Omar Hasan, MBBS, MPH, MS
American Medical Association

Christoph Lehmann, MD
Monroe Carell Jr. Children's Hospital/Vanderbilt University Medical Center

Peter J. Pronovost, MD, PhD
The Johns Hopkins University School of Medicine

Jeanie Scott, MT, (ASCP), CPHIMS
VHA Office of Informatics and Analytics/Health Informatics

Patricia P. Sengstack DNP, RN-BC, CPHIMS
Bon Secours Health System, Inc.

Hardeep Singh, MD, MPH
Michael E. DeBaakey VA Medical Center

Dean Sittig, PhD
The University of Texas Health Science Center

Paul Tang, MD, MS
Palo Alto Medical Foundation

Special thanks to our participating providers and attendees.

Organizations working together with the *Partnership*



©2016 ECRI INSTITUTE



Table of Contents

Partnering for Action: Applying What We've Learned	1
About the <i>Partnership</i>	2
Introduction	
A Need for Health IT Safety Leadership	3
Applying What We've Learned	4
Taking the National Pulse on Health IT Safety	
Prioritizing Health IT Safety Concerns	
Part One	
The Copy and Paste Initiative: Safe Practices Forum	7
Potential Risks and Benefits of Copy and Paste	
The Copy and Paste Initiative: An Evolving Dialogue	8
Appropriate Uses of Copy and Paste	
The Role of Copy and Paste in Communicating Patient Information	
Taking Action Today	
Part Two	
Data Analysis: What We've Learned from HIT Hazard Events	13
Overall Contributory Causes	
Usability	
Local Implementation	
Data Quality	
Decision Support	
Vendor Factors	
Other	
Using Learning to Advance Safety	
Part Three	
Breakout Groups Identify Potential Safety Strategies	21
Rapid Collaboration: Health IT System Alerts	21
Make Alerts Actionable	
Offer an Alternative Path	



Review Systems Data	
Synchronize Efforts	
Rapid Collaboration: Health IT System Banners	23
Standardized Information: to Mandate or Not to Mandate?	
Ensure Information Is Complete	
Delineate Levels of Priority	
The Death of the Banner?	
Rapid Collaboration: Care Delivery Timing	25
Share Information among Caregivers	
Make Timing Visible and Accessible	
Organize Systems According to Care	
Remember the Importance of Communication	
Part Four	
Moving Forward: Analyzing Patient Identification Health IT Safety Concerns	29
Understand the Scope of the Issue	
Define Patient Identification Failures as a Patient Safety Problem	
Clarify Health IT's Role in Contributing to or Preventing Failures	
Identify Promising Technologies, Practices, and Procedures	
Identify Measures for Monitoring Improvement	
Identify Targets for Further Investigation	
Engage Partners in Promoting Intervention	
Enacting Change and Seeing Progress	
References	35
Appendix A: ECRI Institute Health IT Safety Resources	36
Appendix B: Meeting Agenda	37
Appendix C: About Our Speakers and Panelists	39



Partnering for Action: Applying What We've Learned

Dear Colleagues:

ECRI Institute, with funding from the Jayne Koskinas Ted Giovanis Foundation for Health and Policy, is delighted to convene the second face-to-face meeting of the *Partnership for Health IT Patient Safety*. This multi-stakeholder event uncovers ways to advance safety through focused collaboration—making healthcare safer together.

This year's theme, *Applying What We've Learned*, shows that the *Partnership* has come a long way in just one year. Now, the focus turns to solutions arising out of the *Partnership's* collaborative efforts. To that end, we released a first set of Health IT Safe Practices and embarked on developing a second set. We reviewed safety-related events and hazards reported to the *Partnership* and shared our first topic-focused evidence scan. We discussed safety priorities and plans for dissemination of tools that facilitate safe practices.

Most important, our conversation stimulated positive action and enthusiasm. More than 45 participants volunteered for the *Partnership's* second workgroup on patient identification, which shows that by working together, we can create a learning environment in which to accelerate best practices and embark upon improvement initiatives. The *Partnership* will continue to inform a national strategy for health IT (information technology) patient safety, looking not just at the unintended consequences of health IT, but also at the powerful opportunities for using health IT to contribute to and make positive improvements in patient safety. I look forward to sharing these Proceedings with you—and anticipate what the collaborative efforts of the *Partnership* will accomplish in the year to come!

Sincerely,

Ronni P. Solomon, JD
Executive Vice President
General Counsel



About the *Partnership*

The *Partnership for Health IT Patient Safety*, a private-sector initiative, aims to make health information technology (IT) and its use safer through a collaborative multi-stakeholder effort. Convened by ECRI Institute and functioning under the protections of ECRI Institute Patient Safety Organization (PSO), the *Partnership* leverages the work of multiple patient safety organizations (PSOs), clinical users, provider organizations, health IT developers and vendors, an Expert Advisory Panel, and numerous professional societies and organizations to create a learning environment that mitigates risk and facilitates improvement. Reports from the Institute of Medicine (IOM), the Office of the National Coordinator for Health Information Technology (ONC), the Bipartisan Policy Center (BPC), and the draft FDASIA Health IT Report indicate that health IT safety is everyone's responsibility; the *Partnership*, by engaging stakeholders to exchange data on health IT safety issues and identifying opportunities for improvement, facilitates that charge. 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 safer care.

In order to fulfill these goals, the *Partnership* engages in the following activities:

- Establishes a nonpunitive environment for sharing and learning.
- Collects, aggregates, and analyzes health IT-related events, hazards, and near misses from various sources.
- Identifies and shares promising solutions and safe practices.
- Informs policymakers and the broader healthcare community about the barriers and challenges associated with building a safety system for health IT and an eventual center for health IT safety.



Introduction

A Need for Health IT Safety Leadership

As the adoption of health information technology (IT) increases, it opens countless possibilities for the medical community. Patient information can be stored centrally, making that information readily accessible from multiple locations. Medical devices can interface with one another, allowing transmission of records, orders, and additional patient information. Clinical decision support software and safeguards in computerized provider order entry (CPOE) systems can help guide prescribers through the clinical decision-making process and alert them to possible contraindications, concerns, or other risks to the patient's safety. Health IT allows unprecedented ways to examine, aggregate, and utilize patient data, which can lead to improved patient care, knowledge discovery, and safety when used to its fullest potential.

However, the health IT system—its design, implementation, and use—is complex; it involves myriad intricate systems and interfaces. When these systems fail to work or interact properly, a variety of risks can emerge,

posing a threat to patient safety. For example, if notes are simply copied and pasted from one day to the next, the information in the medical record can become overwhelmingly long, and vital patient information can be buried as a result. Too many alerts on CPOE systems can result in alert fatigue, causing caregivers to silence alerts without assessing their validity. And information or orders can be entered into the wrong patient's chart, among other patient identification concerns.

Further, health IT best practices are not always clearly defined. Many facets of health IT safety have not yet been explored. As more healthcare organizations adopt health IT systems, the need for best practices increases exponentially, to further health IT's safe implementation and use.

As a March 2015 Sentinel Event Alert issued by The Joint Commission noted, there are “risks inherent in health IT . . . However, well-designed and appropriately used EHR [electronic health record] systems coupled with strong clinical processes can improve and monitor health care quality and safety

through their ability to access important medical history data, provide clinical decision support, and facilitate communication among providers and between providers and patients” (Joint Commission).

Therefore, the goal of the *Partnership for Health IT Patient Safety* is to identify and share health IT safety learning, best practices, and strategies for success through focused collaboration.

Ronni Solomon, JD, ECRI Institute, described the purpose of the *Partnership* as “making healthcare safer together by establishing a non-punitive environment for sharing and learning.” The *Partnership* achieves this goal by collecting data through a Patient Safety Organization (PSO) structure, by encouraging robust stakeholder engagement and by 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, with the goal of establishing a meaningful national framework for health IT safety.



Specifically, the work of the *Partnership* encompasses several phases:

- **Data collection.** Data collection and aggregation across multiple organizations is crucial. The *Partnership* collects reports of adverse events, near misses, unsafe conditions, and hazards, using standardized formats and nonstandardized data, such as alerts, helpdesk logs, and claims information. The data provide 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.
- **Analysis.** Analyzing the information, from both reported events and evidence scans, facilitates improvements in patient safety and in using and developing the technology. The *Partnership* includes experts in information technology, patient safety, human factors, systems implementation, and healthcare operations, as well as an Expert Advisory Panel. Health IT system vendors serve as analytic contractors under the Patient Safety Act and help analyze the data gathered by the *Partnership*.
- **Collaboration.** Multi-stakeholder workgroups focus on targeted, high-priority topics. They meet regularly, review the evidence, share solutions, identify challenges and barriers, consider product features and

functionality, and create recommendations for safe practices.

- **Leveraged learning.** The knowledge gained through the *Partnership* will be translated into safe practices, recommendations, and tools. Collaborating organizations will broadly disseminate these learnings via publications, at meetings, and through professional organizations, many of which are participants in the *Partnership*. Likewise, endorsement of the *Partnership's* issued practices and recommendations will be sought.

Applying What We've Learned

On October 16, 2015, ECRI Institute convened a face-to-face, multi-stakeholder meeting of the *Partnership*. “Partnering for Action: Applying What We've Learned” was designed to address risks associated with health IT, to define safe practices, and to strategize on how to inform a national strategy for health IT safety. Funded in part by the Jayne Koskinas Ted Giovanis Foundation for Health and Policy, it was the second face-to-face meeting for *Partnership* stakeholders, and included representatives of groups including healthcare providers, health IT developers, academic researchers, PSOs, and professional societies. See Appendix B: Meeting Agenda for the order of the day.

The goals of the day included the following:

- Adopt the *Partnership's* Safe Practices for Copy and Paste

- Establish communications for safe practices
- Launch a new Workgroup on Safe Practices for Patient Identification
- Review the nature and type of safety events and hazards reported to the *Partnership*
- Uncover challenges and barriers to health IT safety
- Agree on which issues are of highest priority for follow-up

Unlike last year's meeting, which was largely an “aspirational meeting,” this year's meeting was a “results meeting,” said Jeffrey Lerner, PhD, ECRI Institute. “We talk about building a culture of safety. Building—it's such an active word. It's a really complex act. And that's what we're doing here. We're building a culture of safety.”

Lerner continued: “A lot of people think you can't do it. They think that the only way we're going to have a culture of safety is if somebody demands it, tells you how to do it.” He addressed *Partnership* participants: “That's wrong. You're proving it to be wrong.”

The *Partnership* underscores the importance of collaboration across all aspects of healthcare and health IT. The *Partnership* relies on its participants, who include representatives from a wide range of healthcare providers, health IT developers, academic researchers, PSOs, and professional societies.

Indeed, collaboration is key, emphasized Solomon, harking back to a quote from Dean Sittig, PhD, University of Texas Health Science



Center, at the 2014 meeting: “We shouldn’t be competing on safety. We want to share [information] about safety so that we can learn from each other’s events.”

Explains Janet Marchibroda of the Health Innovation Initiative: “This [is] a really collaborative day, where we’re all challenging each other to take action.”

Taking the National Pulse on Health IT Safety

Marchibroda spoke of the goals of Capitol Hill policymakers regarding health IT safety, oversight, and advancement. “There’s a lot of agreement on both sides of the aisle [in Congress], and in the private sector, that we need to do this right and we need to move forward,” she said.

However, collaboration is required to determine how best to “move medical innovation forward,” she said.

Andrew Gettinger, chief information officer of ONC, agreed that working together is the best path to health IT safety. When asked outright if he personally thought that a health IT collaborative effort would “make a difference,” he answered that “Forcing [participation via regulation] is the wrong way to go in this space. [Therefore] The collaborative proposed has a much better chance.”

Gettinger went on to present ONC’s proposed Health IT Safety Center as described in a report prepared for ONC, the *Health IT Safety Center Roadmap*. The roadmap outlines steps to be taken in the creation of a national Health IT Safety Center. “We’re proposing something that looks a lot like the *Partnership*,” Gettinger explained.

The first step in developing the proposition for the Health IT Safety Center, he explained, was to convene a task force including health IT safety experts, clinical users, patient advocates, health IT developers, and healthcare organizations. “We came up with some recommendations, and those recommendations are now being evaluated by the U.S. Department of Health and Human Services,” he said.

Goals of the proposed Health IT Safety Center include dedication to shared learning and responsibility, identification and dissemination of solutions, ability to build on private sector initiatives, commitment to those healthcare providers who use health IT as part of their caregiving duties, provision of a space for “private-sector stakeholders and federal government representatives to dialogue and work together,” establishment of a nonpunitive learning environment, and transparency regarding the Center’s operational structure. (“Roadmap”)

To achieve these aims, Gettinger stressed the importance of collaborative learning. He described the ONC collaborative groups as a group of “willing stakeholders,” overseen by an as-yet-undetermined supervisory organization. This will allow “a deeper view of the issue,” he hoped, and noted that information would be received from hazard reports, literature reviews, and research.

More information on the proposed Health IT Safety Center is available at: <http://www.healthITSafety.org>.

Prioritizing Health IT Safety Concerns

The *Partnership* has an abundance of issues to address. Asked to identify the top health IT safety issues, participants responded with numerous concerns, such as usability, culture, interfaces, interoperability, medication errors, noise, and patient identification. See [Figure 1](#). Participants’ Top Health IT Safety Issues for all issues identified by participants.

Figure 1. Participants’ Top Health IT Safety Issues: What Do You See as the Top Health IT Safety Issues?



Participants submitted their primary concerns early in the *Partnership* meeting. The size of each word in the cloud indicates how many times it was suggested: the larger the word, the more participants highlighted it as an issue.



Among health IT initiatives the participants said they were working on in their organizations were the following:

- Data entry burden
- Excessive documentation
- Real-time reporting and analysis

- Transferring information across transitions in care
- Medication reconciliation
- System interfaces
- Alert fatigue
- Patient identification
- Clinical decision support
- Meaningful use

The *Partnership* intends to review and prioritize issues for intensive review via participant input. “At last year’s *Partnership* meeting . . . we decided to create focused, targeted workgroups that looked at high-priority issues and then developed best practices,” said Solomon. The first area of focus that was selected after that meeting was copy and paste.



Part One

The Copy and Paste Initiative: Safe Practices Forum

At the end of the first *Partnership* stakeholder meeting, Partnering for Success, on September 23, 2014, attendees volunteered to participate in workgroups to study why adverse events related to health IT were occurring and to identify best practices to prevent recurrence and promote patient safety. Of the many top issues that were identified during the 2014 meeting, the issue of copying and pasting health information (e.g., orders, notes, labels) was chosen for the first workgroup because of widespread practice and the significant potential for adverse impact on patient safety if copy and paste practices result in the use of inaccurate, irrelevant, or outdated information.

The *Partnership's* copy and paste workgroup convened in February 2015 with Tejal Gandhi, MD, MPH, CPPS, CEO and president of the National Patient Safety Foundation, as its chairperson.

“We defined copy and paste, looked at uses, looked at the literature, reviewed events that had come

into ECRI Institute PSO, talked about vendor functionalities, talked about some best practices from a couple of organizations and how they're working on copy and paste, and then, at the end, got to some recommendations,” said Gandhi of the workgroup meetings.

(For more information on the speakers, see “Appendix C. About Our Speakers and Panelists.”)

The workgroup released safe practice recommendations and a draft copy and paste toolkit, *Health IT Safe Practices: Toolkit for the Safe Use of Copy and Paste*, for review at the October 16, 2015, meeting. This toolkit is available at: https://www.ecri.org/Resources/HIT/CP_Toolkit/Toolkit_CopyPaste_final.pdf. The intent of the copy and paste toolkit is to share information related to the risks and benefits of copy and paste in healthcare and to disseminate safe practice recommendations developed and agreed upon by a multidisciplinary group of workgroup stakeholders to improve health IT patient safety.

ECRI Institute performed a systematic review of the literature to support the workgroup. It is available

at insert: https://www.ecri.org/Resources/HIT/HTAIS_Copy_Paste_Report.pdf. (ECRI Institute “Special Report”) For additional ECRI Institute resources, see Appendix A: ECRI Institute Resources.

ONC's Gettinger highlighted the collaborative nature of the workgroup and the toolkit issued and further reported, “I am delighted with the work that came out of this group.”

Chairperson Gandhi discussed the workgroup's approach and the toolkit in the first session of the 2015 *Partnership* meeting.

Potential Risks and Benefits of Copy and Paste

Copy and paste activities, in part, strive to facilitate efficient medical documentation but have also resulted in new safety risks. During the presentation, Gandhi offered examples of copy and paste activities and potential risks, such as the following:

A physician copies and pastes admission information from another part of the record. Complete imaging study reports and labs, not just abnormal findings, from previous



day's notes were copied into progress notes, thereby making the note "difficult to follow or interpret" because of the volume of information in that note.

As part of the workgroup, feedback was solicited and obtained from *Partnership* members to determine the areas in which copy and paste is often used (e.g., laboratory results, admissions, clinical areas) and the types of information that are most frequently copied and pasted (e.g., notes, problem lists, allergies).

An evidence-based literature review and environmental scan was also performed to further evaluate copy and paste issues. Gandhi stated that although only a few published studies exist on the subject—including one study that indicated that about one-third of copy and paste mistakes contributed to diagnostic error (Singh et al.)—this work will lead to a better understanding about the issues surrounding copy and paste.

Gandhi explained that when developing and evaluating copy and paste recommendations, the group purposefully allowed for flexibility. For example, the workgroup wanted to ensure that vendors would be able to be creative in software and hardware changes, to find innovative ways to address these issues. As such, the workgroup identified the following four recommendations for the safer use of copy and paste:

Recommendation A. Provide a mechanism to make copy and paste material easily identifiable.

Recommendation B. Ensure that the provenance of copy and paste material is readily available.

Recommendation C. Ensure adequate staff training and education regarding the appropriate and safe use of copy and paste.

Recommendation D. Ensure that copy and paste practices are regularly monitored, measured, and assessed. Organizations should evaluate the HIPAA or regulatory implications associated with implementing specific approaches to these recommended practices.

The workgroup recognized that some of the recommendations will take time to implement, particularly those that require technology changes by developers and changes in workflow or usability for providers. Thus, the recommendations were designed to provide a framework by which all stakeholders can implement changes that will positively impact safety. Additionally, the recommendations were designed to allow the stakeholders to identify ways to address these issues as the technology changes, recognizing that external forces, including regulations or compliance initiatives, may impact the recommendations in the future.

The Copy and Paste Initiative: An Evolving Dialogue

Gandhi led a panel discussion about the draft toolkit, asking Lorraine Possanza, DPM, JD, MBE, ECRI Institute, about her vision for the toolkit and how it would be used.

Possanza stated that her hope for the toolkit is that it will help stakeholders to "begin a dialogue of safe practices, so that all of the stakeholders, including frontline staff,

are aware of what the current copy and paste practices are, what the rationale is in using copy and paste, and then how to best maintain the accuracy and reliability of the record when reusing information . . . Often copy and paste is used because systems are not interoperable—lab information does not flow into the record, and so that information is copy and pasted into the record. We really want to think about better and safer uses of the technology. By bringing some of these things to light, you can work with the vendors to really help to innovate other ways for the reuse of information."

Appropriate Uses of Copy and Paste

Brian Crawford, Epic, commented that data can be pulled forward in various ways in addition to the traditional "ctrl + c, ctrl +v" [copy and paste] combination. He stated that the concept of appropriate use of copy and paste is "a really important component of this toolkit." He called the toolkit's recommendation to make copy and paste visible to the appropriate people when needed "elegant." However, he also noted that this concept begs the questions of who needs to see copy and pasted material and when they need to see it "because like most very powerful tools—and I think EHR is a very powerful tool—we have to know what the concept of appropriate use is."

Jeanie Scott, MT, (ASCP), CPHIMS, of the Veterans Health Administration (VHA), indicated that her organization considered what parameters should be enacted for



copy and paste—for instance, when is copy and paste appropriate? Where is it appropriate to display? Who needs to see copied and pasted material?

Gandhi asked Trisha Flanagan, RN, MSN, athenahealth, about how the company's customers typically use copy and paste. Flanagan stated that in her experience, both as an EHR provider and as a former risk manager, copy and paste most frequently occurs in the free text fields. "We tend to see it in the exact [scenarios] that the [copy and paste work] group looked at, to help physicians tell a complex story," she said, "for example, when pulling through a medication list." One participant commented that at the crux of the copy and paste issue is communication—whether copied and pasted information can add something for the patient and family or assist the next provider in diagnostic decision making.

Scott agreed. "That's what ultimately this is all about," she said. "And understanding what we are trying to communicate, how we are communicating it, and whether in paper or electronically—that's just the tool."

Crawford underscored the need to focus on "why people are adding the copy and pasted material. And, then more specifically, what has changed [in the record]" as a result of that action. That is why making copy and paste visible and the provenance of the information available is important: it helps everyone better understand why copy and paste is being used. Flanagan went on to discuss concerns regarding copy and paste activities: "The challenge, really, is the art of telling the story of that patient," she emphasized.

"The answer lies somewhat in being able to pull forward carefully certain information that would prevent a user from ever needing to copy and paste and then being able to edit from there."

Scott further commented that monitoring and auditing copy and paste is not easy. One issue is the sheer volume of copied and pasted data. In 2014, for example, her organization chose to use tracked changes to identify copy and paste material, and found that 90% of every note had at least some copy and pasted material. Identifying the provenance of copied and pasted material is a necessary component of a monitoring program, but what also must be considered is how to set up the system so that staff who are monitoring copy and paste can best do so.

Crawford also talked about expanding this concept from not just identifying that material was copied and pasted, but other information, such as the interface or system from which it originated. "So that's really what we're trying to focus on then, is that bigger picture. Can we capture where all the pieces came from? Can we tell that story over time in a meaningful way so that we're presenting the right information to the right people at the right time?"

Scott also acknowledged the difficulty in monitoring and auditing effectively, sharing that her organization has pulled back somewhat on audits after finding that their efforts affected system performance—the system was slowed significantly. "I think the key part that came out of the [workgroup] recommendations

was the monitoring, the measuring, [and] the assessing."

Gandhi also asked Scott about "never use" scenarios for copy and paste and how that plays a role in the VHA's policy and system. Scott stated that these are mostly for note documentation and provided the example of one "never" event for copy and paste: the signature block. "You wouldn't put someone else's signature block on your check, so why put it on a note?" Scott asked.

Scott also discussed limits on other sections in the note, such as not allowing previously recorded data into the record if it's not needed for the encounter (e.g., the entire lab findings versus the pertinent results). The reason behind the limits is "note bloat," in which notes become so long, due in part to copied and pasted material, that they are no longer a useful communication tool.

Another item Scott offered to the group for consideration is the next stakeholder who will begin to use notes: patients and families. Indeed, there have been projects that allow patients to read their notes, so there is a need to be cognizant of how patients will engage and interact with their notes. "[We need to] think forward—why are we copying and pasting [information]?" asked Scott. Gandhi expressed hope that the tools contained in the copy and paste toolkit would get others thinking about these questions.

The Role of Copy and Paste in Communicating Patient Information

Michael Victoroff, MD, Lynxcare, addressed the issue of copy and



pasted material as it relates to medicolegal concerns. Although, as Victoroff noted, “We don’t see notes unless something is wrong.” He used his medicolegal perspective to pose a patient safety question: Is the documented information adequately informing the reader and appropriately telling the story? Adding out-of-date, irrelevant, or redundant information to a note can obscure clinically relevant information (Weis and Levy). Victoroff recommended that metadata (e.g., timestamps) associated with copied and pasted material should be visible only when appropriate and available on an as-needed basis.

A discussion about whether copy and paste has actually been proven to be helpful ensued. Possanza commented that the evidence scan and review of the empiric and gray literature “did not yield a lot of data to associate copy and paste with adverse events or with specific advancements in clinical care. Most of what the studies have shown is that anecdotal evidence exists for this practice. We’re . . . at the tip of the iceberg, recognizing and beginning to look at the issue from a safety perspective.”

The advantages and disadvantages of copy and paste are discussed in the toolkit; Gandhi stated that the issue now is to learn how to use copy and paste safely. The safe practice recommendations move us in that direction.

Another topic discussed during the panel was how to best engage customers in identifying ways to improve

copy and paste and clinical documentation issues.

“What we [Epic] try to tell our community members is ‘we want to know when stuff goes wrong,’ ” said Crawford, who acknowledged that it can be difficult to distinguish health IT and other issues. “But whenever we even have a hint of copy paste-related issues, or anything else like that, you need to protect yourself and do your due diligent investigation within your own organization. But even if we aren’t involved from day one, we want to know what happened,” stressed Crawford.

For Flanagan with athenahealth, early engagement with users during development helps them to identify problems. She believes the vendor community can improve both its efforts and offerings by understanding the “how” and “why” behind copy and paste activities: “Where is the application lacking?” she shared that her organization seeks

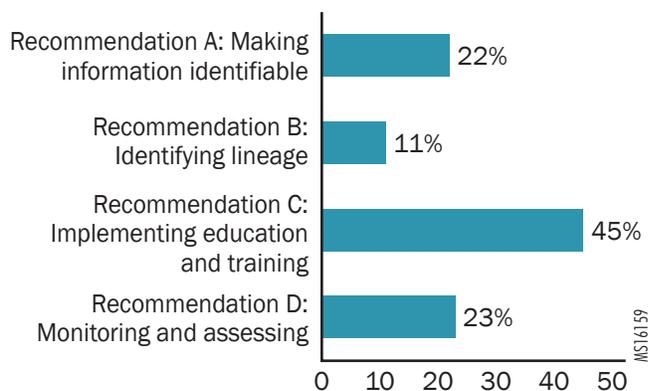
to understand. “What could we do, what could we configure in a way that [the interface] could have more structure?” Flanagan asked, with the hope of identifying ways to reduce the reliance on copy and paste.

Taking Action Today

Following the copy and paste panel discussion, *Partnership* participants were asked to weigh in on which recommendations they could apply within their own organizations. Answers were submitted via an anonymous polling platform. The results can be found in [Figure 2](#). Actionable Steps for Participant Implementation. Most respondents believe that they could most readily implement Recommendation C— Ensuring adequate staff training and education regarding the appropriate and safe use of copy and paste.

Participants were also asked whether they had any other recommendations for the safe use of copy

Figure 2. Actionable Steps for Participant Implementation



Participants reviewed the action recommendations presented by the copy and paste workgroup and selected those options they believed they would be most able to implement within their own organizations. Most selected “implementing education and/or training,” saying they could do so fairly quickly, while fewer believed that monitoring and assessment practices and making copied-and-pasted information identifiable were immediately achievable goals. Few participants believed that their organization could identify the lineage of copied and pasted material without additional resources or support.



and paste. Participants responded with the following:

- To eliminate it completely
- To standardize how copied and pasted material is made visible
- To block copying of the signature block
- To remember the purpose of documentation as a communication tool

- To use copy and paste sparingly—only when it helps communication
- To directly observe use of copy and paste
- To design systems to make copy and paste unnecessary

These and other ways to implement safe practice recommendations for copy and paste

are addressed in *Health IT Safe Practices: Toolkit for the Safe Use of Copy and Paste* available at: https://www.ecri.org/Resources/HIT/CP_Toolkit/Toolkit_CopyPaste_final.pdf.



Part Two

Data Analysis: What We've Learned from HIT Hazard Events

Robert C. Giannini, BS, NHA, CHTS-IM/CP, ECRI Institute, presented an overview of a subset of *Partnership* data collected in 2015. “Every event I look at has a different twist, a different nuance,” he said.

Specifically, Giannini worked with a sample of *Partnership* data to determine what healthcare information technology (HIT) information can be gleaned using the HIT Hazard reporting taxonomy, developed from the Agency for Healthcare Research and Quality (AHRQ) HIT Hazard Manager. The HIT Hazard taxonomy allows reporting about precursors to events: hazards. Giannini explained these hazard fields and provided specific event examples from reports. The reports use the HIT Hazard form, which was developed using the HIT Hazard Manager Taxonomy (Walker et al.).

The HIT Hazard taxonomy includes additional fields that are not in the AHRQ Common Formats. The information collected using this

taxonomy, which ECRI Institute PSO has incorporated into its reporting system, provides greater detail about the discovery and contributory causes of health IT events and hazards, as well as remedies for them.

Between July 2014 and May 2015, six healthcare organizations submitted a total of 152 reports using the HIT Hazard form. (Note: none of the fields in the form are required, so totals may vary from chart to chart, depending on how users filled in the form for each event.)

The first of the fields looks at who discovered the issue and how it came to be reported, as seen in [Figure 3. How Events Were Discovered](#). Most of these events were discovered and reported by the end user (the person using or familiar with the technology)—then typically reported as an event or hazard to someone in the risk, quality, or IT departments, specified Giannini.

Another finding highlighted by Giannini: most events are found during production (i.e., the actual use of the system during patient care); few were identified during testing or the initial go-live phase. This is

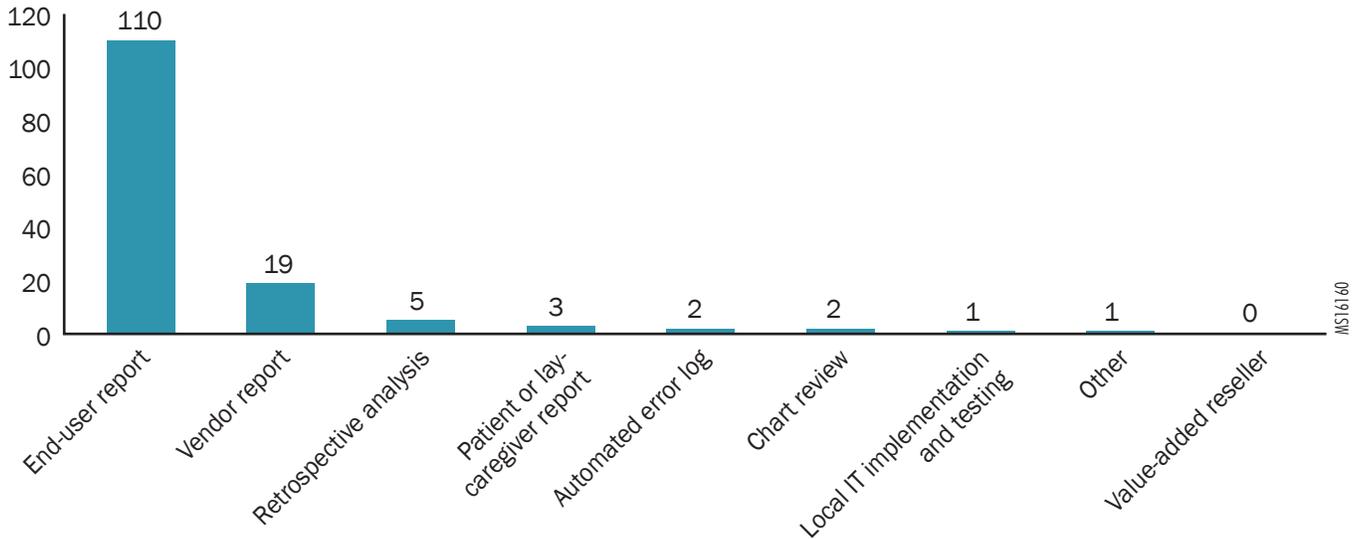
in part because events would not necessarily be reported during those phases but are much more likely to be reported when the technology is being used for everyday activities. See [Figure 4. When Events Were Discovered](#) for more information.

When Giannini reviewed the communication chain for each event, though, he found something surprising. Of the events, 116 “were only communicated internally. [The report] went to IT, it went to patient safety, it went to risk,” he said. “Only 20 were reported to the software vendor.” (See [Figure 5. How Events Were Communicated](#).) One could speculate that this could be in part because no outside vendor actions were required, with local IT addressing the issue. However, this may also indicate a missed opportunity for vendor notification, which might lead to the creation of improvements in the technology. For more analysis of the events reported to the vendor, see [Drill Down: Events Reported to Vendor](#).

Giannini then compared all events to those reported to the vendor. “For a majority of the events, most things

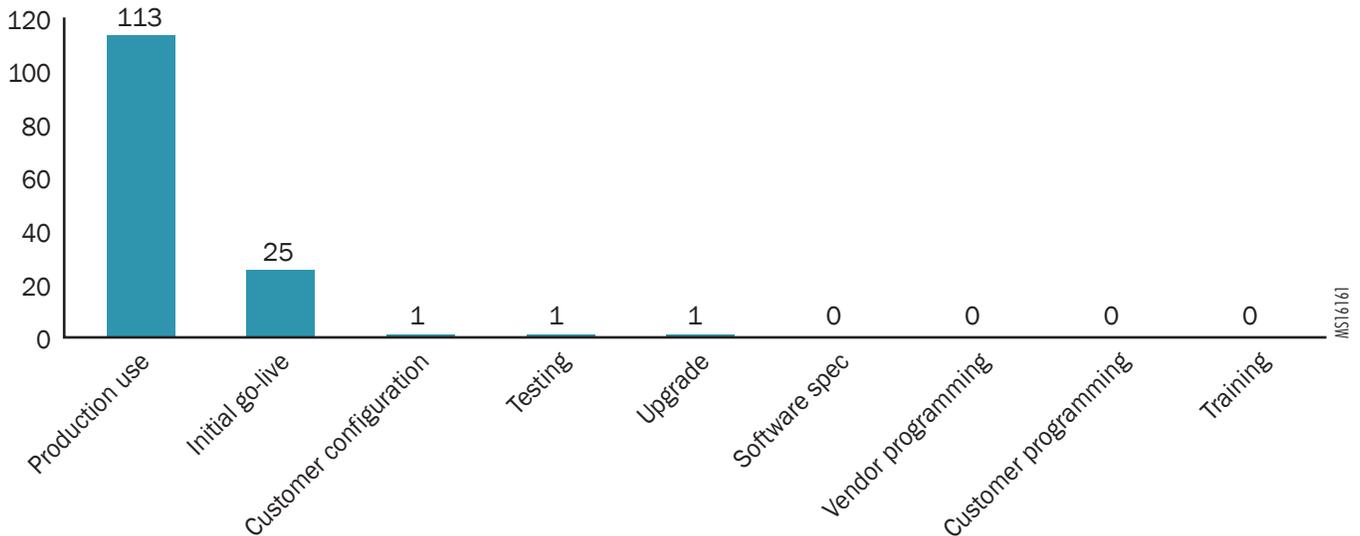


Figure 3. How Events Were Discovered



Most events reported using the HIT Hazard taxonomy were identified via end-user report. Other sources include vendor reports, retrospective analysis, patient or lay-caregiver feedback, automated error logs, and chart review.

Figure 4. When Events Were Discovered



Most events were discovered during daily use of the health IT system, as opposed to during the initial go-live phase, configuration, or testing.

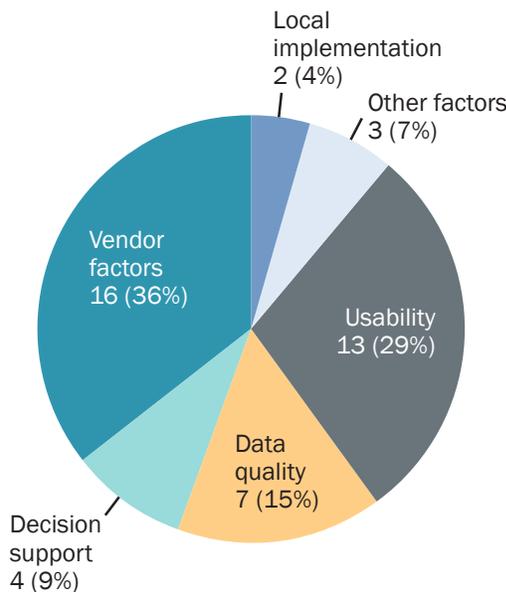
DRILL DOWN: EVENTS REPORTED TO VENDOR

Giannini drilled down specifically into the subset of events reported to the software vendor. For these 20 events, Giannini reviewed the contributory causes tagged to each event (in the HIT Hazard taxonomy, fields are optional, and events can be tagged with multiple factors). See [Figure 15](#). Contributory Causes of Events Reported to Vendor. Most common were the classifications of usability and vendor factors—these two items would help to better align the system with organization workflow or would allow for more rapid access to information. Decision support, data quality, and local implementation concerns were much more infrequent in those events reported to the vendor.

It is understandable that provider organizations may not have the inclination, time, or resources to report problems that they are able to fix on their own. It is also understandable that vendors want to focus on the problems that they can fix. What remains unknown is whether the absence of sharing these problems inhibits the design of safer or more reliable products. Perhaps the *Partnership* can play a role in gathering and sharing these types of events.

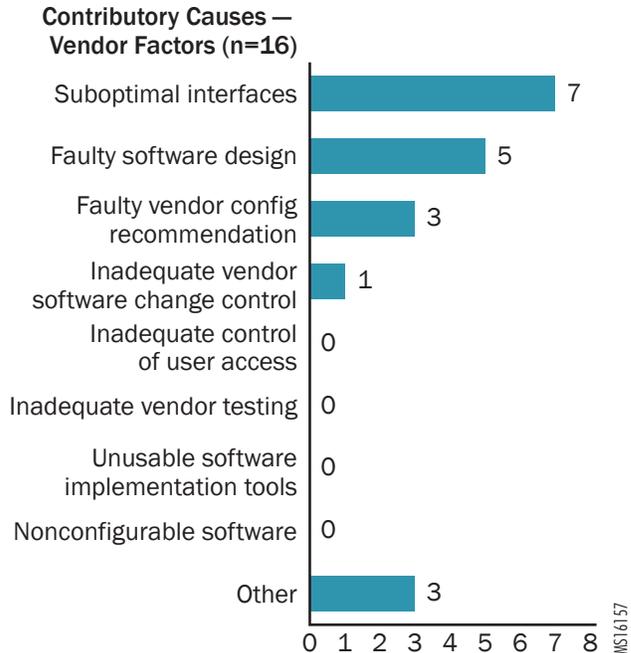
Vendor factors, the largest contributory cause category, merited further analysis. These 16 events revealed that interface issues were most common, followed by faulty software design, vendor configuration, and inadequate vendor software change control. Information reported to vendors is frequently limited to issues for which vendor intervention, such as a permanent software fix, is required. However, increased reporting to vendors may increase opportunities for safety advancement. See [Figure 16](#). Vendor Factors Events Reported to Vendor.

Figure 15. Contributory Causes of Events Reported to Vendor (n = 20)



The 20 events reported to the vendor were tagged with factors from different contributory causes. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

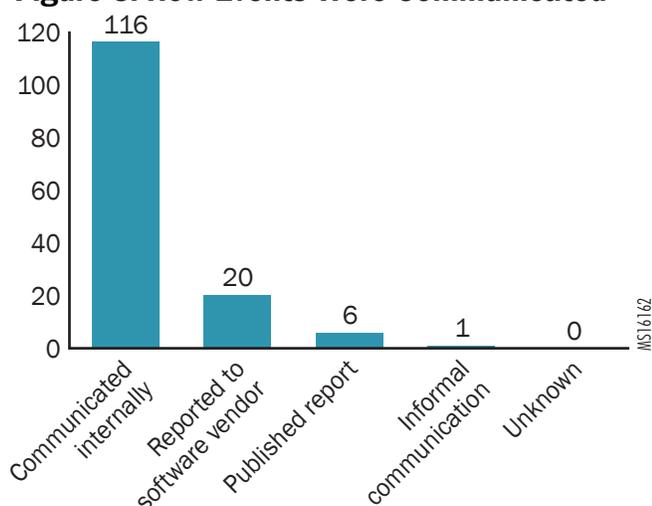
Figure 16. Vendor Factors Events Reported to Vendor



The 16 events reported to the vendor that were tagged with "vendor factor" contributory causes indicated that interface issues were most common, followed by software design issues and configuration concerns. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)



Figure 5. How Events Were Communicated



Most events are communicated internally; few events were reported to the software vendor.

Table. Control Steps Taken in All Events versus Events Reported to Vendor

First Control Step	All	Reported to Vendor (n = 14)
Local IT configuration change	46	1
Training for end user	32	2
Vendor software fix	19	11
Local IT custom programming	12	1
Other	11	5
Training for local IT	3	
Policy change	2	
Care-process change	2	

Much of the follow-up to the events reported to the *Partnership* involved local IT configuration or custom programming changes as well as training for those using the technology. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

are being fixed at the local configuration level,” he explained. Other local solutions included software training for staff, custom programming by local IT staff, policy changes, or changes in care process. [Table. Control Steps Taken in All Events versus Events Reported to Vendor](#) provides information about how the events were addressed and whether

specific modifications or changes were made.

Overall Contributory Causes

The HIT Hazard taxonomy allows the reporter to provide information about the contributing causes of hazards. See [Figure 6. Event Contributory Causes by Type](#).

Usability

Overall, usability (i.e., disruption of workflow and difficulty finding or entering information) was the most common contributing factor entered by those reporting using the HIT hazard taxonomy (events could be tagged with multiple contributing factors). Options associated with usability in hazard reporting include the following:

- Confusing information display
- Mismatch between actual workflow and health IT workflow
- Mismatch between health IT capabilities and user expectations
- Difficult data entry
- Inadequate user feedback from the system
- Hard-to-find information

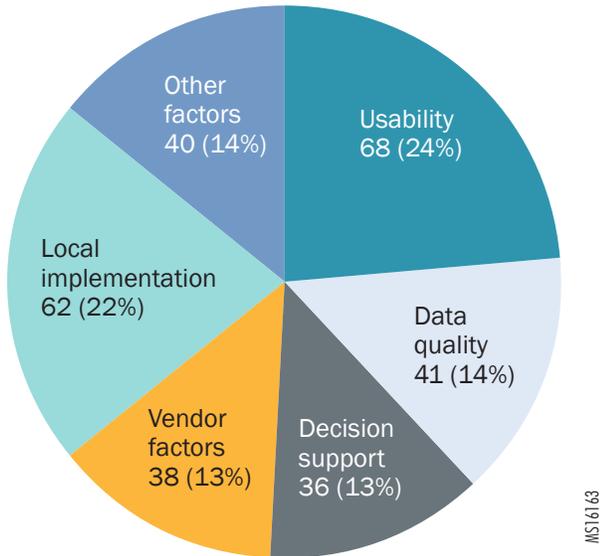
Reported hazards or events often involved several subcategories within usability. These factors were self-identified by the reporting facility, not by the analytic staff at ECRI Institute PSO. See [Figure 7. Usability as a Contributory Cause](#).

A report on confusing information display stated:

In two events, an extra medication dose was given to the patient. In each instance, the medication had been ordered as a one-time order and administered the day before the duplicate dose was received. Even though the administration of the medications was documented on the medication administration record, the documentation of this action was not readily visible to the staff.

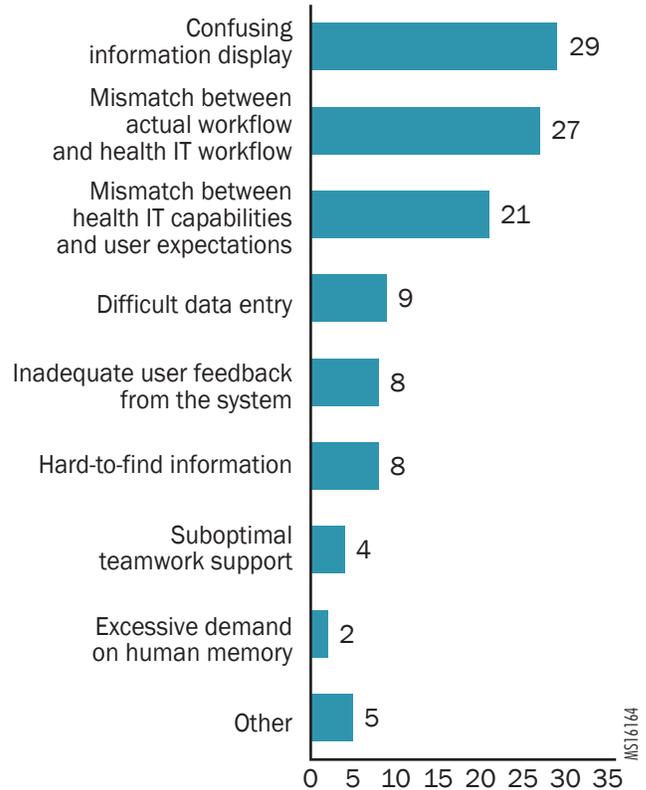


Figure 6. Event Contributory Causes by Type



Overall, usability was the most common contributory cause of reported events. Local implementation, other factors, and vendor factors were also common. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

Figure 7. Usability as a Contributory Cause



Of the 68 events pertaining to usability, confusing information display and mismatched workflow expectations were most common. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

Another report demonstrates how differing workflows between the health IT system and the organization's practices can result in potential safety issues:

A patient was transferred between hospital units. During the electronic medication reconciliation of an order for prednisone, which was being given in a tapering dose and was ordered to be continued upon transfer to the new unit of the facility, the dosing regimen was started over from the beginning. The patient received an extra day of the higher dose before this was discovered.

Other contributory causes involving usability include local

implementation—the next largest category reported—data quality, decision support, and vendor factors.

Local Implementation

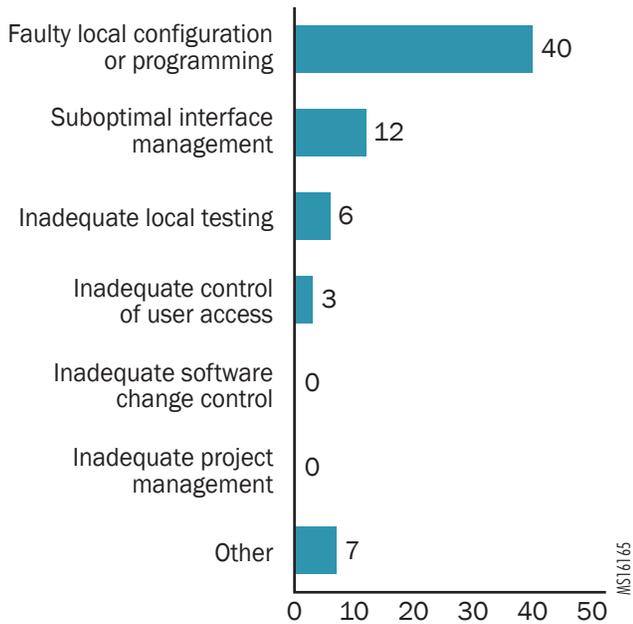
The local implementation category of contributing causes includes such factors as faulty local configuration or programming, suboptimal interface management, inadequate local testing, and inadequate control of user access. See Figure 8. Local Implementation as a Contributory Cause.

One report explained that the system was not adequately configured to meet the needs of the patient and provider or to facilitate workflow:

The patient underwent a surgical procedure. The provider ordered three doses of an intravenously administered antibiotic to be given every eight hours. The order for the postoperative antibiotic was entered, and the pharmacist verified the order. The first dose should have been given following the procedure. However, this did not occur; instead, the patient did not receive the medication until the next day. It was later discovered that based on the system's order start time date/time logic, the medication was not received on the day or at the time it was intended.

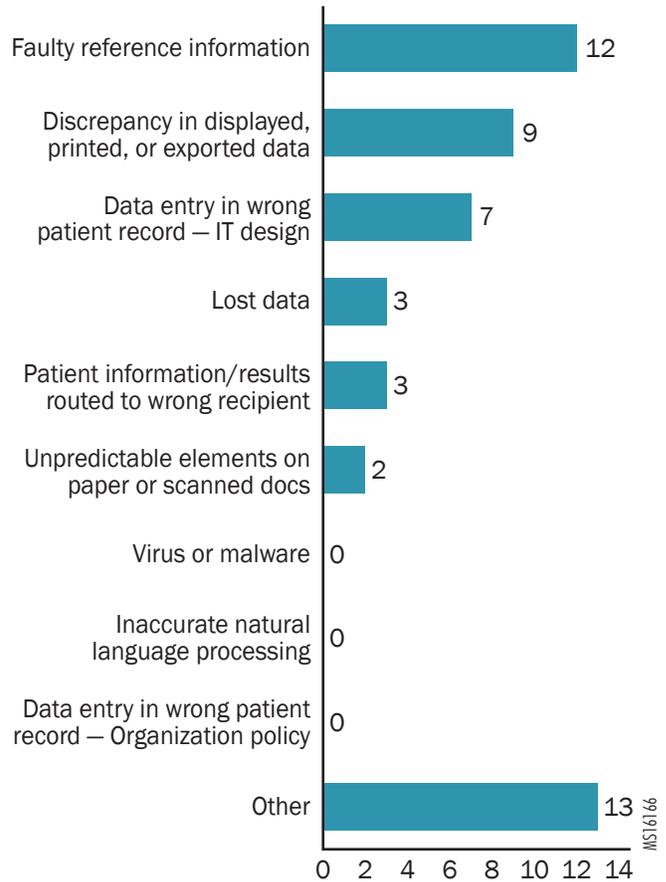


Figure 8. Local Implementation as a Contributory Cause



Of the 62 events related to local implementation factors, most common was faulty local configuration or programming, while interface management was next most common. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

Figure 9. Data Quality as a Contributory Cause



The 41 events related to data quality demonstrate the risks that can result from faulty reference information, data discrepancies, and incorrect or lost data. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

Issues with order and task-performance timing continue to appear in events reported to the Partnership.

Data Quality

The data quality category of contributory causes includes faulty reference information; discrepancy in displayed, printed, or exported data; and other factors. See Figure 9. Data Quality as a Contributory Cause.

Examples of data quality issues demonstrate the safety risks of poor search capabilities and character limits (e.g., the confusion that can arise resulting from such limits):

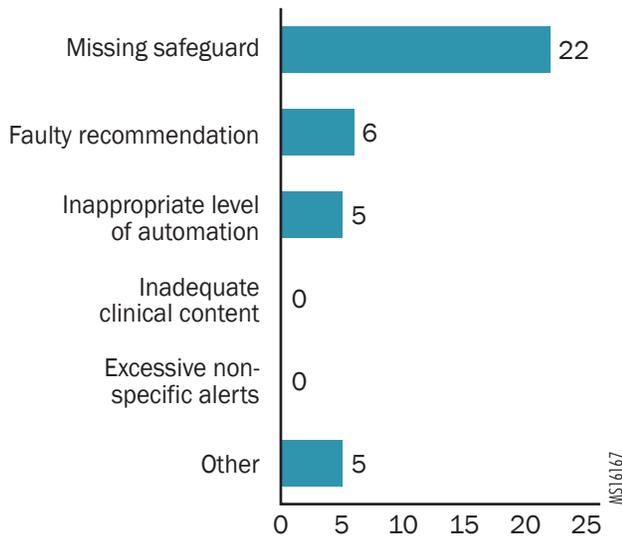
- *When ordering an Epi-Pen, a keyword search for this medication only brings up the pediatric dose option and does not indicate that the adult dose is available. There is the concern that an inappropriate dose could be inadvertently ordered for an adult.*

- *The reporter noted that when data was being entered into a flowsheet, system users were prohibited from entering all of the characters of text they were attempting to enter as the row no longer populated text once the threshold of data characters was reached.*

Both of these events demonstrate hazards, rather than actual safety events; neither reached a patient, but both have the potential to cause harm. Distribution of this learning

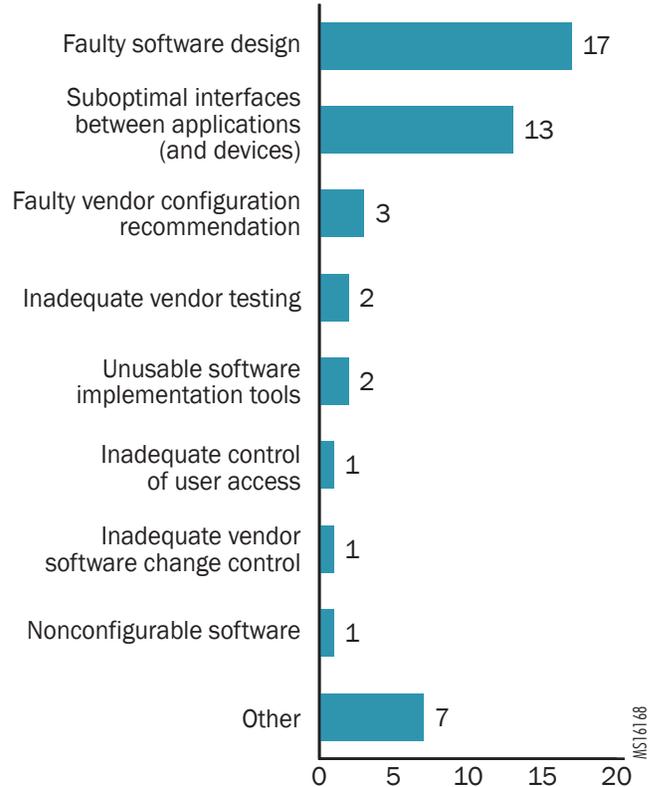


Figure 10. Decision Support as a Contributory Cause



Of the 36 events reported related to decision support, missing safeguards were most common, followed by fault recommendations, automation level, and other concerns. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

Figure 11. Vendor Factors as a Contributory Cause



Of the 38 events reported related to vendor factors, faulty software design, interface concerns, and configuration recommendations were common. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

prevents those actual safety events from occurring.

Decision Support

Giannini reviewed events that were reported as examples of decision support issues. Decision support includes alerts for safeguards and additional clinical information to enhance clinical decisionmaking and improve workflow; see Figure 10. Decision Support as a Contributory Cause for the full list.

For example, events reported under this category reveal that clinical decision support notifications may be overlooked by providers. One

report indicated that multiple practitioners may have been bypassing alerts, while two others highlighted problems involving inaccurate patient records:

- *Toradol and Motrin were given together. [These medications are not to be used in combination and typically a warning is displayed if the medications are ordered/appear together.] Because the patient received both of these medications together, there was concern that the physician (who ordered the medication), the pharmacist (who filled the order), and the*

nurse (who administered the medication) had bypassed alerts.

- *The physician was able to enter an order on the record of a discharged patient, which could lead to misplaced or incomplete orders and inaccurate patient records.*
- *An organization noticed that merging a patient's chart led to an overlap of allergy information—one chart showed an allergy, but the other showed no known allergies.*

Vendor Factors

Within the vendor-factor category of contributory causes, events were



attributed by reporters to faulty software design, interfaces between systems, configuration recommendations, vendor testing, and more. See [Figure 11](#). Vendor Factors as a Contributory Cause.

“How do you deal with changes made in the system downstream?” Giannini asked the meeting participants. “For example: when a lab order is amended—how does that information get to the other systems that it interfaces with? How does the technician collecting the sample know that the order has changed?” In such issues, risks pertaining to interoperability and flow of information are especially common. Both remain challenges for provider organizations, as seen earlier in the meeting when participants shared their safety concerns (see [Figure 1](#). Participants’ Top Health IT Safety Issues).

In one example, these suboptimal interface and use issues did not become apparent until providers interacted with the system:

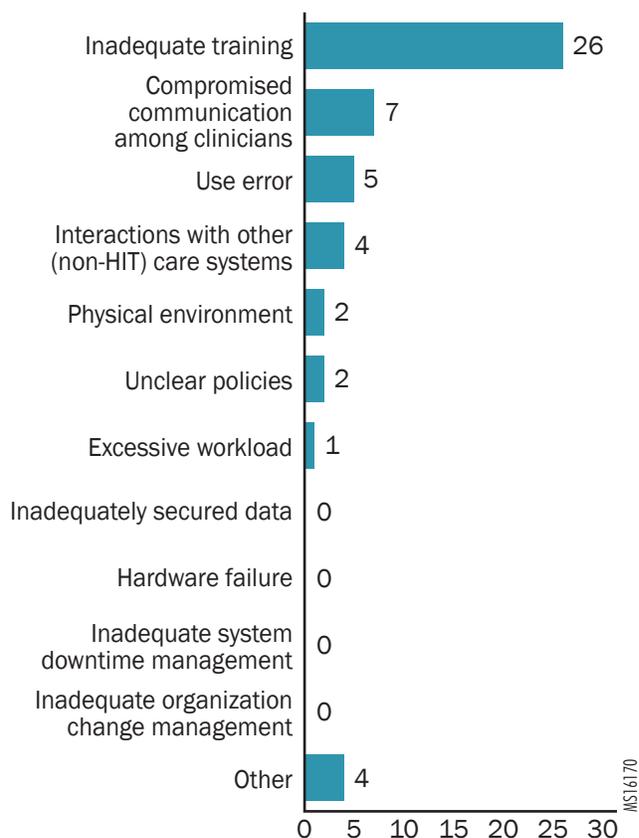
When multiple patient charts were open, alerts and alert responses might not actually fire for the correct patient record.

Other

Events reported as “other” hazards include inadequate training, communication, use error, non-health IT system interaction, physical environment, unclear policies, and excessive workload. See [Figure 12](#). Other Factors as Contributory Causes for more information on these.

Technology has changed workflow, and oftentimes, the visible clues that were present in paper records (e.g., thickness of the color, ink chart, location on page) are no longer relevant or present. So, when distractions and interruptions caused

Figure 12. Other Factors as Contributory Causes



Of the 40 events reported related to other factors, training was the most common concern. (Note: Users of the HIT Hazard taxonomy can fill out multiple fields per event, and each field is optional.)

by the fast-paced clinical environment occur, additional hazards exist.

Using Learning to Advance Safety

“Identification of health IT events and hazards is not always easy or apparent,” noted Giannini. Sometimes, the role of the health IT systems in patient safety events can be difficult to identify, when the focus may be on more overt event factors or outcomes. Likewise, added Giannini, “the majority of health IT hazards are only communicated internally.” Organizations should continue to help those using the technology to recognize hazards,

which can lead to safety events, and to report not only those issues that lead to events, but also those issues that could lead to events. As seen in the data, few issues were reported to the vendor. Issues were frequently resolved internally. By not communicating outside the organization, opportunities for learning were lost. Moreover, vendors are deprived of firsthand insight regarding the needs of providers; therefore, new functionalities are unavailable to address those universal needs. All stakeholders need to be involved in reviewing and implementing mitigation strategies.



Part Three

Breakout Groups Identify Potential Safety Strategies

During the *Partnership* meeting, participants split into multi-stakeholder focus groups to identify strategies for combatting the risks of three common health IT pitfalls: system alerts, EHR page banners and headers, and timing issues. Each of the three topics was represented by two actual scenarios, which were dissected by different groups, and then all participants shared their concerns, experiences, learning, suggestions, and recommendations with the meeting participants. The group members aimed to answer a series of questions: What should be happening in this scenario? What is the reality? What are some short- and long-term approaches for vendors and healthcare providers? What strategies can be implemented to reduce risks in each scenario?

Rapid Collaboration: Health IT System Alerts

Scenarios:

- Oftentimes patients are on medications prior to a change

in orders. In other instances, multiple providers are ordering the same class of medications but have ordered different drugs. In some instances, patients are on multiple medications from the same class of medications. Alerts are intended to make providers aware that there may be a conflict, such as two medications from the same class, medications that are not appropriate for the particular patient, or incorrect dosages. In this example, the anticoagulants heparin and rivaroxaban were ordered, verified, and administered. Two individuals, at various times, overrode the alert notifying them that there was duplication. Both overrides stated the same justification: "benefits outweighed the risks."

- *Multiple medications were dispensed to a patient. The medications that were ordered were both beta blockers. In some instances this may be acceptable, while in others, this would create a problem for the patient and alerts would notify the provider about possible*

duplication. In this case example, Lopressor 25 mg PO Q12 h was ordered and verified on Thursday. The first dose was given on Thursday at 2100. Several days later, on Sunday, Coreg 3.125 mg PO BID was ordered and verified, and the first dose was dispensed on Sunday at 1700. The patient received doses of both beta blockers within hours, receiving Lopressor on Sunday evening and Coreg on Monday morning. The event report included the following comment: "This problem should have been caught at multiple stages in the medication process. It is noted that MDs do not see alerts for duplicate medications when they are ordering medications."

Participants in the alarms focus group agreed that the process of prioritizing alerts and notifications safely is daunting. One participant used the metaphor of a guard dog: "You don't want a guard dog that never barks or that always barks. You want the one that barks when someone wants to break into your house."



Another participant continued the metaphor and emphasized the use of additional strategies—not just system alerts. “I don’t want a guard dog, but I want a fence and other security measures. I want a guard dog only if I can’t build a fence,” clarified the participant. “There is a place for alerts, but they should be the last thing; if you have to choose to have it, your vendor should [help you be able to] sunset that alert as soon as possible.”

The alerts focus group participants offered several recommendations:

- Make alerts actionable and accurate.
- Use alerts to offer alternatives.
- Review alerts usage and system data.
- Share learning and coordinate efforts.

Make Alerts Actionable

“The alerts need to be accurate and actionable,” one participant stated.

Another participant worried that the reasoning behind alert selection and use contributes to alert fatigue: “Too many times, clinicians get irrelevant information. Clinicians need useful information. It all comes down to ‘clinically relevant information in a timely manner’—the information I need, when I need it.”

Other participants agreed. “For example, I have an outpatient, but I see the patient’s inpatient medication list, and it’s so irrelevant to the current situation,” explained one participant. “Medications can be buried in the middle of a list or go unseen. How do we approach that?”

However, determining when information needs to be visible is a daunting task. One participant noted that “there are different levels of expertise, and the question on how we think about alerts must be keyed to who will be facing those alerts—for example, a medical assistant, a nurse, or a physician.”

In this vein, participants noted that some organizations allow specialists the ability to filter out certain alerts, although others prevent alerts from being filtered out. As one participant explained, “We decided not to allow filters in our organization. The theory for the alert is that you forgot. We don’t think you don’t know it, we just think you forgot.”

Likewise, alert severity should be customized, as well as alert presentation, suggested participants. Who will see the alert? Does it show up as the order is being written? Does it show interactions, and if so, does it provide a chance to learn more about the other order? Or, as one participant suggested, should the alert present differently based on the type of action? For example, this participant noted, “there are drug [dosage] range alerts, but I want a different looking alert when I do a tenfold over or under dose.”

Participants also worried that once created, alerts remain in the system far past their usefulness. “The alerts that we’re building today may not be relevant in six months,” said one participant, “but we don’t turn them off.”

Choosing which alerts to set is an “enormous task,” one participant said, explaining that the organization sometimes becomes frustrated. “We

had to make the decisions because no one else would stick their neck out and say, ‘Don’t pay attention to this.’ The liability keeps shifting down the line until it becomes a decision by the nurse or the doctor.”

Another participant noted a similar concern: “Alerts generated during order entry . . . are piled onto the pharmacist, and that’s dangerous.”

Not all alerts are useless, though. For example, two participants shared experiences with actionable alerts: one was set up for women of childbearing age not to receive certain medications without taking a pregnancy test, and another was a reminder for the practitioner to tell patients on birth control pills being prescribed erythromycin that the medication would affect their birth control’s effectiveness.

Still, concluded participants, “Many alerts aren’t actionable,” as one participant complained. “It’s an alert for a reason, but there’s no ‘so what?’ factor. Sometimes it’s just not clear, and you have to go back to make sure you have all the patient-specific information to make sure you’re making the right decision . . . Don’t give me paragraphs on the drug interaction; tell me the bottom line.”

Offer an Alternative Path

Therefore, participants considered whether the format of the alert might make it more valuable. For example, would an alert be more useful if it were “to say ‘your patient may bleed out,’ rather than ‘you have scheduled two anticoagulants?’” asked one participant. Highlighting the results of the alerted action rather than the action itself may lead to



stronger clinical decisions, agreed participants.

Likewise, participants posited that responses to alerts may be more useful if clinicians had the ability to select why they were overriding an alert—for example, adding “thank you for the reminder,” or “I did not need this alert” when noting that the benefit of a medication outweighs the risk, as in the event above. Standardized feedback options could allow for more in-depth system analysis or event review.

Review Systems Data

When considering the value of the alerts created within the system, one participant noted, the “good catch” rate should be reviewed—“How many times did clinicians change what they were going to do? If you have 2,000 good catches come from 200,000 alerts, that’s only 1%.” Another avenue to be explored for alert review includes audit trails, suggested one participant. Another recommended trending the alerts that are dismissed, overridden, or turned off, explaining that the organization this participant represents performs such analysis annually in an effort to reduce alert fatigue. We look at “which alerts are on, which are used, which are overridden, and what the decisionmaking process is,” the participant explained. However, another participant commented, “What is an acceptable override rate? It’s not really black and white.”

Other participants suggested that seeking input from system users, such as physicians, may be beneficial. “What are physicians

expecting?” one asked. “In one case, a resident said that the first thing they told him when he started was to ignore all the alerts because they’re not applicable.”

Therefore, when assessing system alerts, the culture of the organization should be assessed as well. As one participant remarked, “No one ever wants an alert to fire for themselves; they only want them to fire for someone else.” Supporting a culture of safety and learning can help to smooth such reactions from clinical staff.

However, although duplicate orders are often frustrating to providers and contribute to alert fatigue, participants agreed that they should not universally be turned off. “There are many reasons why you might want to allow these duplicates,” they stressed, such as increasing the likelihood that an alert is seen.

Synchronize Efforts

Therefore, efforts regarding alert function should be synchronized, determined participants. “Would a national framework to share [alert format] help?” asked one participant.

Another participant noted that even among vendors, tiered alerts are not standardized, which can lead to confusion. “None of them are coordinated,” the participant explained.

Organizational planning could also support system review and modification, suggested a participant, who expressed concern that healthcare organizations see only the surface costs of implementing a health IT system and don’t budget appropriately for maintenance and upkeep.

Participants also emphasized the role that order sets can play in reducing alert fatigue. “If I devised a protocol for drug-drug interactions, I don’t need to see [the alert], because the order set takes care of it,” explained one participant. “Default order sets help reduce alerts, but they have to be up-to-date, credible, and usable.”

Rapid Collaboration: Health IT System Banners

Scenarios:

- *In many EHRs, a colored banner or header appears and contains a set of information. Included in that set of information may be the patient’s name, allergies, date of birth, or other information that is deemed to be something that should be readily visible. Because the amount of information that needs to be in the header may vary, not all of the information is always visible. In some instances, care providers must hover over the information with a mouse or cursor to obtain more detailed information. However, sometimes hovering is not enough and the care provider must also click on that information to obtain the full text. In this event, the patient header showed allergy information. However, for this patient, it was only able to contain partial allergy information. More information was made available upon hovering, but when hovering over the allergy section, the complete list was still not revealed. It was only if*



the care provider knew to click on that allergy information that the total list of this patient's allergies would be revealed.

- *In some banners, a medical record number is displayed. This information may be used by other departments to keep track of results, route results appropriately, or capture billing items that are used during the patient visit. In this case example, the medical record number was used to direct blood glucose results that were routinely taken on patients before meals so that the information would populate directly into the chart. Typically, the testing can be done twice a day; sometimes it is done more often. In this case example, when completing morning glucose testing, the staff member inadvertently entered the visit number [this was a number that appeared on their task list]; they did not enter the patient's medical record number. This incorrect entry resulted in the test results not appearing in the medical record.*

Banners in patients' health IT system files pose several challenges for healthcare providers and organizations. A limited amount of "real estate" is available, so only the most important pieces of patient information can be part of the header. As one participant said, pieces of information should need to "fight their way" onto the banner. Moreover, the value placed on each piece of information differs among types of

providers, care facilities, and even among individual clinicians.

Therefore, a significant challenge exists in determining how to present information in the banner that is useful, accurate, and complete. Discussion of participants' experiences with and modifications of headers in their own organizations quickly brought a critical issue into specific focus: Are headers best suited for patient identification only, or are they also appropriate for other information that must be immediately available?

The banners group offered its recommendations:

- Consider standardizing banner information, but remember that different practitioners need different information.
- Ensure that information on the banner is shown in its entirety.
- Delineate levels of priority for information to be shown in the banner.
- Search for comprehensive alternatives to the banner.

Standardized Information: to Mandate or Not to Mandate?

Banners and headers may be the first place in a patient's EHR that providers look to for information, but inconsistency in what's displayed there and how it is represented can raise the risk of all sorts of errors when providers work in multiple practices or locations—or even on multiple units within a single hospital.

Participants from two different health systems described their approaches to deciding what can

be included in banners. One system largely standardizes banner information in its inpatient settings, but allows affiliated physician practices significant freedom to customize the system in their own practices. By contrast, a second system described an opposite approach, enforcing standardization across all of its inpatient and outpatient locations.

Noting that the goal of the banner should be to provide "information that is useful, accurate, and complete," an EHR vendor explained that its banners are not configurable. Banners should contain only information "that is of such sufficient import that everyone who sees that patient needs to know," such as a patient's picture, name, date of birth, and do-not-resuscitate (DNR) status, the vendor stated.

Ensure Information Is Complete

Including too much information in the banner runs the risk that some of it might go unseen by the provider. The organization runs the risk of providing only a partial picture, when providers don't realize there's more to the story, noted one participant, suggesting that it would be better to give the user nothing.

Participants discussed the importance of including complete and unambiguous information in banners. For example, if a patient's allergy information is included in the banner, it should include all of the patient's allergies, not just a partial display—otherwise, users may assume that they are seeing all of the information and not realize that some has been cut off. To



that end, fields should be set to contain only the maximum number of characters that can be displayed, recommended one participant: “We need to set limits. If we’re going to [use a] hover [feature], then limit the display to the number of characters that can display when you hover.” Participants agreed: shortcomings in consistency and completeness cannot be overcome by user training alone, although one participant did comment that their organization provides a help desk for physicians that is staffed by registered nurses 24 hours a day.

Such risks are revealed when users must click an information button or take another additional step to view the rest of the banner’s contents. “It doesn’t matter how well you train someone, no one is going to always remember” to perform that action, commented one participant.

Making decisions about information to be made present in system banners is often difficult. While, as one participant noted, “everyone wants everything” in the header, it becomes unwieldy and ineffective when too much information is included.

Delineate Levels of Priority

Participants discussed which items might be of value to the practitioner and therefore be included in the banner. In addition to name, date of birth, and medical record number, possible items include:

- Code status
- Advance directive
- Infection control/isolation status

- Vaccinations
- Non-English speaking
- Payer

However, further exploration is clearly needed to develop best practices and standards for determining and managing pieces of information that need to be “immediately available.” As one participant stated, “Facilities would not bring in a new medication without evaluating it through their formulary committee. The same rigor is needed for EMR [electronic medical record] decisions.”

The Death of the Banner?

Finally, participants discussed whether the very idea of a banner or header—a visual holdover from paper records—was “self-defeating” and unnecessarily constrained. Taking advantage of all of a computer’s capabilities, some noted, could include abandoning a rectangular or tabular display and moving toward a 3-D model of patient information that reflects the patient’s clinical setting and situation.

Such a system would provide contextual information “just in time” based on the clinician’s needs. For example, a provider performing a procedure may need to see and confirm a patient’s blood type. But if that patient collapses before the procedure even begins, the provider will more urgently need to know the patient’s DNR status, and blood type will be a secondary concern. A more responsive, less spatially limited display could allow the user to pivot more quickly between tasks based

on the patient’s frequently-changing condition.

Rapid Collaboration: Care Delivery Timing

Scenarios:

- *Antibiotics are commonly needed during dialysis. In the paper world, repetitive orders were generally understood; however, with electronic ordering it is not always clear when orders start and stop, and because of that, orders may be missed. In this case, antibiotics were ordered “after dialysis.” Even though the patient underwent dialysis multiple times per week, only one dose of the medication was dispensed. The intention was for the medication to be received after every dialysis treatment.*
- *In orthopedic surgery, antibiotics are often given prior to the start of a procedure, right after a procedure, and then another dose of the antibiotics are given in an appropriate interval, resulting in three doses. It is important that the doses are received in a timely manner to achieve the maximum effectiveness of the antibiotic administration. In this case example, a patient underwent an orthopedic procedure, and the provider ordered antibiotics (cefazolin 2 g IV q8h x 3 doses). The pharmacist verified the order. The doses of the antibiotic should have continued immediately after surgery;*



FOCUS GROUP RECOMMENDATIONS: TAKE ACTION

Alerts

- Make alerts actionable and accurate.
- Use alerts to offer alternatives.
- Review alerts usage and system data.
- Share learning and coordinate efforts.

Banners

- Consider standardizing banner information, but remember that different practitioners need different information.
- Ensure that information on the banner is shown in its entirety.
- Delineate levels of priority for information to be shown in the banner.
- Search for comprehensive alternatives to the banner.

Care delivery timing

- Share information among caregivers, ensuring that all are aware of the patient's current status as needed.
- Improve visibility and accessibility of dosing delivery times.
- Organize systems according to the care being given.
- Remember that technology does not replace communication.

however, based on order start date/time logic and the time that the order was entered into the system, the start date was changed to the next day and the patient did not receive the antibiotics in a timely manner.

“We first identified that the issue of timing is incredibly complex, that the use cases are enormous, and . . . we believe that there is a need to develop a list of use cases of everything that can go wrong with timing, and work from there backwards, and look for solutions, because just like the problems are very complex and different, the solutions will [likewise] be different,” said one participant.

The literature and learning shared by other organizations can be a valuable source of information to form a list of priority timing issues. For example, suggested one participant, the ordering process requires an explicit start time—but timing can vary across multiple institutions for practitioners who travel among them. Likewise, the participant noted, it should be clarified when the first dose will happen and who needs to know such information. Participants suggested several tools and strategies, such as visual prompts, aids, or dashboards.

The care delivery timing focus groups suggested the following recommendations:

- Share information among caregivers, ensuring that all are aware of the patient's current status as needed.
- Improve visibility and accessibility of dosing delivery times.
- Organize systems according to the care being given.
- Remember that technology does not replace communication.

Share Information among Caregivers

Participants suggested that developing a “shared mental model” would allow all providers involved in a patient's care to see the whole process for a patient's care. Once providers write an order, they often don't know what happens to it afterwards, noted one participant. Therefore, the information about a patient's care must be visible to all those involved in the patient's care (e.g., providers, nurses, pharmacists) so everyone is equally aware.

Another participant noted an experience involving a “protocol coordinator” staff member—each staffer was assigned individually to a patient with the goal of making adjustments to the patient's chart or communicating to the patient's care team as needed.

However, participants raised the questions of replicating this function within the EHR. Why not create a “super menu” of all things happening to the patient in a consolidated view for the patient's care team



members to access so they can adjust the patient's care needs based on changing information?

Another area of timed care delivery that could benefit from such tools as a dashboard or patient tracker, suggested participants, is events with conditional timing, such as the administration of a medication after a procedure. As one participant suggested, a dashboard or patient tracker could use a timed event, the patient's location, or the notification (e.g., the patient is in the OR or has undergone an MRI) as a trigger for any necessary timed care delivery.

One presenter noted, "What we've currently identified is [that] this is at the interface of policy, workflow, and technology, and one of the things that is required is that institutions spend a significant amount of time actually thinking through the issues . . . because these are incredibly complex items [without] simple solutions."

Other participants noted that families and caregivers should be provided with information so that their insight can help provider better care for the patient.

Make Timing Visible and Accessible

Multiple participants discussed the concept of a "visibility tool," such as an in-EHR calendar, to make timing needs more accessible, visible, and easier to comprehend.

One participant shared the experience of placing rules on timing for certain drug classes. Without such rules, the participant noted, the physician might order a medication with

instructions for the first dose to be administered "right now," with no idea as to the exact administration time.

Other participants worried about people's ability to recall dates. One concern with timing is that dates can mesh in a person's mind. It's hard for humans to differentiate a date when it is presented in writing or verbally just as Oct. 16 or Oct. 17, for example. However, a calendar display makes the day and date more easily visible.

Another participant noted concerns regarding stop dates and times. The EHR system in use at this participant's organization doesn't allow future stop dates to be entered, which has forced clinicians to use a workaround. This participant worried about the "illusion that what's put in the computer is being communicated." Instead, this participant emphasized, "This information needs to be part of the handoff."

Likewise, pharmacy staff do not always see information regarding timing; health IT screens and views are not always the same for providers and pharmacists, noted one participant. Participants agreed: the ordering system needs to be interoperable with pharmacy.

Likewise, participants expressed concern that reliance on the free text field in the health IT system leads to instances of missed information. To this end, provider education may also play a role in ensuring that the health IT function supports the workflow, suggested participants.

Organize Systems According to Care

One vendor participant is working to address timing concerns by attaching orders to where the patient is in the care process. The goal is to trigger certain time-critical needs as patients transition through each step of their care.

Participants discussed this concept; one noted that for dialysis patients, the trigger could fire when the patient leaves dialysis and activate the necessary order sets.

Remember the Importance of Communication

It's important to recognize that computers cannot replace all communication, stressed several participants. Sometimes, they stressed, the care team members need to actively reach out to one another to communicate important information, and likewise, care team members have to ensure that hand-offs are effective.

For example, one participant noted, not all inpatient and outpatient EHR systems exchange data or communicate with each other. So, a patient's elective surgery may be arranged in an outpatient setting, but the inpatient system cannot receive the necessary instructions, such as the timing of antibiotic administration before surgery, so the information is faxed to the inpatient facility instead, and that information can get lost.

Likewise, participants reiterated that the care team cannot rely solely on prompts from the electronic



record. “If you make it too configurable, you can get in a danger zone,” one participant warned. “It cannot replace the human element.” For

example, there is a risk in simply assuming that an electronic hand-off will happen. For some high-risk scenarios, the care team needs to

meet face to face rather than rely on electronic communication about the patient.



Part Four

Moving Forward: Analyzing Patient Identification Health IT Safety Concerns

The stakeholder meeting served as a launching pad for a new *Partnership* workgroup, addressing safety concerns with patient identification. “Our goals are basically to define patient identification failure as a patient safety problem and clarify health IT’s role in either mediating those errors or, hopefully, preventing them,” said William Marella, MBA, MMI, ECRI Institute. The workgroup will also identify promising technologies, practices, and procedures and develop measures for improvement.

“We’ve had literally thousands of patient identification reports come in to ECRI Institute PSO,” said Marella. “The scope of what we’re going to try to do [in the Patient Identification Workgroup] is to focus on the breakdowns in that process, which is basically what we’re getting adverse event data on.” (See [Figure 13](#). Patient Identification Group Process Map.)

Understand the Scope of the Issue

“I know who my patient is. Why do I have to ask them again?” This question, reported by panelist Lori Paine, RN, MS, Johns Hopkins Medicine Armstrong Institute for Patient Safety and Quality, underscores the fundamental dilemma of how to ensure accurate patient identification in an increasingly complex and fast-paced environment of care. Also, given tension between clinical (e.g., safety, quality) and administrative (e.g., efficiency, productivity) demands, a disconnection can exist between the pressures on frontline healthcare providers and the imperative to verify such basic information at the beginning of each patient interaction.

The critical nature of human involvement in patient identification—despite the ever-growing role and capabilities of technology in the process—was evident throughout the panel discussion. One panelist found the amount of human decision making involved in patient identification, regardless of the systems or technologies used, “striking.” Another panelist asserted that, due to decades-long

normalized deviance in healthcare, the system itself has led practitioners to develop habits that put patients at risk for identification errors.

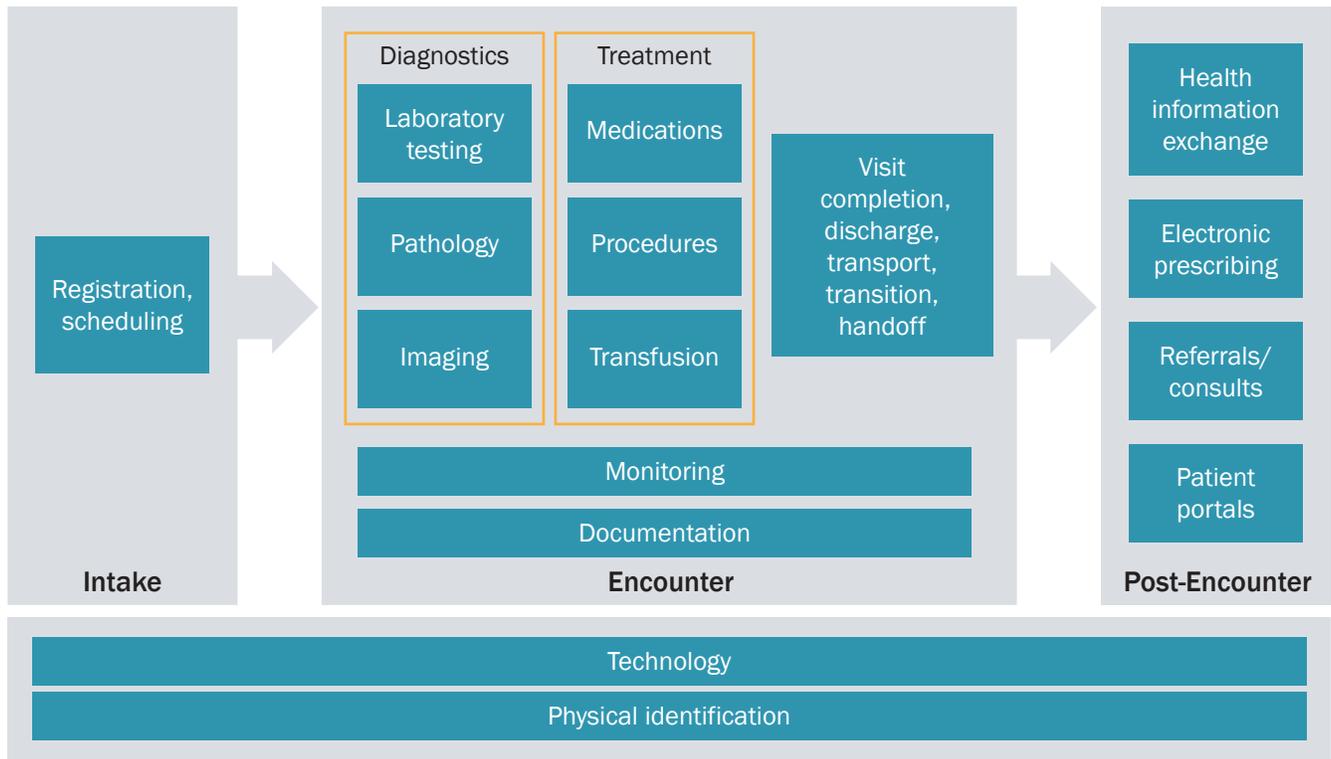
At the conclusion of a spirited and candid discussion involving a wide variety of stakeholders, the workgroup’s charge was clear: because a wide variety of challenges contribute to the problem of patient identification errors, the ultimate solution must be multifaceted.

Define Patient Identification Failures as a Patient Safety Problem

Marella described his initial exposure to failed patient identification practices in the healthcare industry. Ten years ago, he shared, the Pennsylvania Patient Safety Reporting System (PA-PSRS) received a report of a patient who inadvertently received a spinal injection when she mistakenly walked into a pain management practice instead of a nearby dental office; after she received the injection, the patient remarked, “this seems like a lot to get my tooth fixed,” and the provider realized that the woman was not the patient she had been assumed to be.



Figure 13. Patient Identification Group Process Map



The patient identification group intends to follow patient identification processes from registration through diagnosis, treatment, follow-up care, and more. One participant observed that closing the loop should be an important part of the process, so that any errors identified are not permitted to recur.

Since that time, Marella noted, there have been thousands of additional reports of patient identification errors reported to ECRI Institute PSO.

This incident, and the subsequent variety of patient identification errors discussed by the panelists, quickly brought the broad nature of the issue as a patient safety problem into focus. Examples ranged from a patient who was physically in the wrong place at the wrong time, to multiple patients in the same “place” (a single provider’s computer screen) at the same time.

Adopted from the Australian Commission on Safety and Quality in Healthcare, the workgroup’s working

definition of patient identification is “the process of correctly matching a patient to appropriately intended interventions and communicating information about the patient’s identity accurately and reliably throughout the continuum of care.” (ACSQH)

Panelist Terhilda Garrido, MPH, ELP, Kaiser Permanente, added that the challenges of patient identification are broad and “absolutely have safety implications.” Accordingly, defining and managing the scope of the initiative is a critical initial task for the workgroup.

There is also an entrenched cultural component of normalized deviance in healthcare, Paine

posited, which manifests itself in the context of patient identification when clinicians resist verifying a patient’s identity because they are certain that they have the correct patient.

In anticipation of the workgroup’s efforts, preliminary work has included the development of a process map to categorize the points in the continuum of care at which a patient identification error can occur, including the following:

- **Intake.** Intake issues may occur before the patient is even physically present for care, such as during scheduling or registration.



- **Encounter.** Besides physical identification, encounter safety concerns encompass those that may occur during hands-on aspects of care such as diagnostics, treatment, and documentation.
- **Post-Encounter.** Post-encounter events may occur in activities such as electronic prescribing and use of health information exchanges.

Clarify Health IT's Role in Contributing to or Preventing Failures

Many participants' comments illustrated how health IT can contribute to patient identification failures; some hinted at how it may help prevent them.

For example, panelist Jason Adelman, MD, MS, New York-Presbyterian Hospital/Columbia University Medical Center, discussed capturing events during which a practitioner places an order on one patient's record, cancels it, and places that order on another patient's record. "That's a very good marker," he noted.

However, Adelman explained, orders comprise only a small subset of all patient identification errors.

Other error categories noted by Marella include mislabeled lab specimens, ordering tests for the wrong patient, and reporting test results to the wrong patient. Marella shared that ECRI Institute PSO sees a variety of patient identification errors throughout the continuum of care from registration and scheduling to diagnostics, treatment, and

monitoring. For example, orders have been initiated for the correct patient but documented in an incorrect patient's record, monitors have been placed on the wrong patient, and test results have been pushed to the wrong EMR. In the preliminary data, diagnostics were the leading event type and ranged from mislabeled specimens to tests performed on the wrong patient.

Garrido shared that she was motivated to dig deeper on patient identification safety concerns when, in the course of a sentinel-event review, she realized that an emergency room physician had four electronic charts open at the time a drug was erroneously ordered for the wrong patient. Strategies discussed by participants for such a situation include verifying the patient's initials, date of birth, and a third identifier before continuing.

She also discussed the challenges faced by large systems serving large populations; in such circumstances, it's typical to have many patients with the same name, and the duplicate identifiers don't necessarily end there. For example, she shared, Kaiser Permanente has identified 36 individuals with the same name living in the same city in southern California.

Indeed, throughout the discussion panelists acknowledged that many patient identification scenarios require multiple strategies (e.g., algorithms, photos, re-verification) to ensure patient match.

Sharing a finding that had surprised him and his colleagues, Adelman stated that the cause of patient identification errors isn't as

intuitive as one might expect. For example, the researchers had anticipated that the majority of electronic wrong-patient errors were the result of juxtaposition (e.g., a physician intended to place an order on Mr. Smith but placed it on Mr. Jones instead). (Adelman et al.)

However, they found this was true only about 10% of the time. Rather, 80% of electronic errors were attributed to disruption (e.g., getting a call that Mr. Jones needs pain medication while working in Mr. Smith's record).

Garrido likewise reported that she hears a "cacophony of observations" on erroneous information getting into the wrong patients' charts, and that the sources of these errors are many and varied. The concordance in patient identification that one might expect does not exist, even in a closed system, such as Kaiser Permanente, in which there are close links between provider and payer, she shared.

Rather, Garrido finds that many challenges remain in identifying the correct patient and medical record. Everyone wants to move quickly, she says, and a significant identification failure can occur even before the patient arrives at the registration desk. Moreover, such issues will multiply as health information technology continues to evolve, she worried.

Identify Promising Technologies, Practices, and Procedures

Panelists had many suggestions for improvement, with general consensus around the need for a multifaceted, system-wide solution.



Paine suggested that the workgroup's process map (see [Figure 13](#). Patient Identification Group Process Map) is "missing an arrow"—the one at the end that closes the loop so that organizations have better ways of knowing what has occurred and not letting the error back into the system.

Mark Segal, PhD, GE Healthcare IT, concurred and added that he was struck by the complexity of the map. Patient identification, he noted, "really begins and ends with what human beings do." This includes ensuring the accuracy of how fundamental information such as name and date of birth are recorded, because inputting the best possible data into an EMR will lead to more confident conclusions. He emphasized the importance of appropriate standards and organizational policies for accomplishing this task, and acknowledged that unless clinicians receiving data via a health information exchange are willing to rely on it, enter it, and incorporate it into a record, it has little value.

Segal noted that, despite the critical importance of algorithms for matching, he was struck by how much human decision making is involved in patient identification. For example, decisions must be made about how to tune algorithms, whether to worry more about false positives or false negatives, and how to identify and resolve exceptions. Segal cited the recent release of certification regulations from ONC, which defined a minimum set of data elements for information sent through a health information exchange and constrained how they can be created,

and noted that the regulations provide a "useful benchmark" for the industry to follow.

However, acknowledging that much more research is needed, Adelman believes that the "ultimate solution" for patient identification will be multifaceted, with multiple photographs, validation, and reverification. Citing emerging research in the pediatric arena, for example, Adelman shared that photographs appear to support patient identification in children's hospitals, and that his team recently demonstrated that use of a distinct naming convention reduced identification errors in the neonatal intensive care unit at Montefiore Medical Center, Bronx, NY (Adelman et al.).

Garrido likewise cited a few strategies that may prove beneficial: a unique identifier, use of photo identification (including having patients upload their own photos), and patient access to records, such as through Open Notes, which allows patients to detect and correct misinformation. She is certain that a "system-wide solution," including patients, providers, administration, and other resources is needed to address the broad challenges of patient identification.

Paine called for the workgroup—and the industry at large—to look outside of healthcare and analyze industries that are leaders in identification. Referencing aviation specifically, Paine acknowledged that it's "easier said than done," but that the healthcare industry needs to broaden the environment for solutions to other industries that are using technology to better secure identifiers.

Comparing the two security environments, "we're just not at the same place," Paine said of healthcare, noting that identification processes in airports are very different from what they are in healthcare facilities.

Regarding the impact of health insurance exchanges on data integrity, Garrido specified that ensuring patient match is indeed a challenge in a health insurance exchange, but hopes that exchanges will highlight the broader problem and motivate the healthcare industry to jointly develop best practices so that providers will ensure that they are working with the correct patient. She referenced Kaiser Permanente's example of 36 individuals with the same name living in the same city as an example of the need for algorithms to help confirm patient match and also to illustrate the potential of photo identification and biometrics.

Acknowledging widespread concern about the role of government in a national patient identifier initiative, Marella asked the panel about the conditions necessary to make a national patient identifier politically and technically feasible. Segal responded that this initiative was actually part of the Health Insurance Portability and Accountability Act; however, since 1999 there has been an annual prohibition against funding promulgation of a federal standard for a national patient identifier. Therefore, implementing a national patient identifier would require either changing federal law or changing interpretation of federal law. Also, Segal explained, although having a consistent unique identifier would likely lead to a greater



than 99% match rate, it could not be relied upon to achieve high and consistent matching without other strategies. For example, he stated, patient identifiers are used in Europe, but only in conjunction with other patient matching methods.

Marella asked panelists: “Are there opportunities to standardize the methods providers are using to identify patients accurately?” Panelist Hardeep Singh, MD, MPH, Michael E. DeBakey VA Medical Center, responded that “huge opportunities” exist; however, most people he has spoken with have not even heard of existing clinical practices and resources, such as the SAFER guides, available online at <https://www.healthit.gov/safer/safer-guides>.

Singh advocated building on the existing evidence and cautioned that stakeholders should be careful not to “shoot for the moon in trying to do something in the near term, and get bogged down with so many other types of issues, such as sort of political deliberations that we don’t have control over.”

Holding that “the system itself” has created patient identification problems, Paine referenced the Human Factors Analysis and Classification System (HFACS), used by the military and the aviation industries, and its applicability to error analysis in healthcare. She suggested that the application of HFACS could lead to better understanding of the long and varied roots of patient identification, which she called “as much technical as they are adaptive.”

She emphasized the importance of telling clinicians about cases in which very simple mistakes were made at one or more points and engaging frontline staff in learning how to solve them. She also cautioned the group against “addressing symptoms instead of root problems,” as well as overlooking the special issues faced by organizations with an international patient population.

Identify Measures for Monitoring Improvement

Adelman discussed the current state of the research on patient identification, recognizing that there is a dearth of data and much opportunity for learning. “It seems that I’m going to be spending my career on this one issue,” he joked, “and I think it’s going to take multiple careers until we ever really solve this problem.”

Adelman referenced the “retract and reorder” tool that he and colleagues were able to identify and implement. “But,” he emphasized, “ordering is just a small part of where all the wrong patient errors are happening, and for the vast majority of things in the patient safety world, we don’t have the good fortune of having a measure that works perfectly.”

Identify Targets for Further Investigation

Participant discussion repeatedly returned to how many screens, or electronic charts, a provider should be able to access simultaneously. Singh acknowledged that consensus on this issue has not been reached and that tradeoffs exist, balancing safety with efficiency. Garrido agreed

that health IT offers many beneficial efficiencies for busy clinicians, and that there is a need to balance efficiencies and safeguards.

One participant reflected that he heard panelists discussing two different issues: actual, physical wrong patient versus computer errors in patient matching. Even with 99% or greater probability of a correct match, the potential for misidentification is important, he added.

Another participant broached the topic of medical identity theft and proposed that problems with patient identification can be managed “to an extent” in the care environment. However, he stated, when addressing malicious interference with a record, vetting and reconciliation of false information (e.g., wrong blood type, medication that was never administered) is a major challenge.

Engage Partners in Promoting Intervention

Chaired by Hardeep Singh, MD, MPH, the patient identification workgroup had its first meeting on November 20, 2015, and will issue its recommendations mid-2016.

The workgroup intends to focus on breakdowns or gaps in the patient identification process as identified by adverse event data received and investigated by ECRI Institute PSO, which has already started to investigate such events. ECRI Institute has published risk management guidance on patient identification (see Appendix A: ECRI Institute Health IT Safety Resources for more information on these).



Marchibroda noted that patient identification is a “hot topic” for a variety of stakeholders, including the College of Healthcare Information Management Executives (CHIME), the Healthcare Information and Management Systems Society (HIMSS), and the Bipartisan Policy Center (BPC)—all of which have been making significant efforts toward developing effective strategies.

Ronni Solomon, JD, acknowledged that the first task of the workgroup is to define the scope to keep the initiative manageable and achievable. In the coming months, the workgroup will continue to focus on clarifying health IT’s role in patient identification and developing promising technologies, practices, and procedures. Participants will also begin to engage partners in promoting interventions shown to improve patient identification and work towards identification of additional measures for monitoring improvement and priority targets for research and development.

Enacting Change and Seeing Progress

At the conclusion of the *Partnership* stakeholder meeting, participants were again polled on what they think the top health IT safety issues are. See [Figure 14](#). Today’s Top Health IT Safety Issues for more.

Figure 14. Today’s Top Health IT Safety Issues



At the end of the meeting, participants were asked to describe the three issues they perceive to be today’s most pressing health IT safety concerns.

The concluding discussion focused on how to disseminate best practices, shared strategies, health IT safety learning, and other resources among all healthcare organizations. Suggestions made include town hall meetings, online publication and communication, joint policy statements, and pilot-testing of *Partnership* recommendations in participant facilities.

One participant commented that “As far as disseminating best practices, I think it needs to happen at multiple levels, starting within individual organizations, of course.”

However, expanding such sharing can be a challenge even within an organization, this same commenter noted: “When one site figures out something that is a challenge—or something they do really well—we have the challenge of disseminating it throughout the other sites within that single organization.”

Nevertheless, progress is evident. “Looking back where we were a year ago, we’ve made tremendous progress,” the participant noted. But “one of the big challenges of healthcare policy is getting people to do things without regulating that they [have to] do things . . . That’s something to keep in mind when we think about the path forward: If it was easy, it would have been done already.”

Solomon emphasized the capabilities of the *Partnership* and reminded participants that its strengths stem directly from the efforts and input of all involved. “By working together,” she said, “we create a learning environment in which to accelerate best practices, embark upon improvement initiatives, and make meaningful improvements to patient care and safety. That’s why we’re here.”



References

- Adelman J, Aschner J, Schechter C, et al. Use of temporary names for newborns and associated risks. *Pediatrics* 2015 Aug;136(2):327-33. Also available: <http://www.ncbi.nlm.nih.gov/pubmed/26169429>
- Australian Commission on Safety and Quality in Healthcare (ACSQH). Patient identification. Available from Internet: <http://www.safetyandquality.gov.au/our-work/patient-identification/> (cited Nov 2015).
- ECRI Institute. Special Report: Copy/paste: prevalence, problems, and best practices. 2015 Oct 1. Available from Internet: <https://www.ecri.org/resource-center/Pages/HIT-Safe-Practices.aspx> (cited Nov 2015).
- Joint Commission. Safe use of health information technology. Sentinel Event Alert 54. http://www.jointcommission.org/assets/1/18/SEA_54.pdf (cited Nov 2015).
- ONC. Health IT Safety Center Roadmap. 2015 Jul 17. Available at: <http://www.healthitsafety.org/uploads/4/3/6/4/43647387/roadmap.pdf> (cited Nov 2015).
- Singh H, Giardina TD, Meyer AN, et al. Types and origins of diagnostic errors in primary care settings. *JAMA Intern Med*. 2013 Mar 25;173(6):418-25. Also available: doi: 10.1001/jamainternmed.2013.2777. PMID: 23440149
- Walker JM, Hassol A, Bradshaw B, et al. Health IT hazard manager beta-test: final report (AHRQ Publication No. 12-0058-EF). 2012. Rockville, MD: Agency for Healthcare Research and Quality. Available from Internet: <http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf>
- Weis JM, Levy PC. Copy, paste, and cloned notes in electronic health records. *Chest*. March 2014;145(3):632-8. Also available: <http://dx.doi.org/10.1378/chest.13-0886>. PMID: 24590024



Appendix A: ECRI Institute Health IT Safety Resources

- 2015 Top 10 Patient Safety Concerns for Healthcare Organizations.* Available at: https://www.ecri.org/components/HRC/Pages/RMRep0415_Focus.aspx
- 2016 Top 10 Health Technology Hazards.* Available at: <https://www.ecri.org/Pages/2016-Hazards.aspx>
- Alarm Safety Resource Center.* Available at: <https://www.ecri.org/alarmsafety>
- Copy/Paste: Prevalence, Problems, and Best Practices. Available at: https://www.ecri.org/Resources/HIT/HTAIS_Copy_Paste_Report.pdf
- ECRI Institute PSO Deep Dive: Health Information Technology.* Available at: https://www.ecri.org/components/PSOCore/Pages/DeepDive0113_HIT.aspx
- ECRI Institute PSO Deep Dive.* Laboratory-related Safety Events. Available at: <https://eshop.ecri.org/p-171-pso-deep-dive-laboratory-related-safety-events.aspx>
- ECRI Institute PSO Deep Dive.* Medication Safety Events. Available at: <https://eshop.ecri.org/p-142-pso-deep-dive-medication-safety-events.aspx>
- Guidance Article: Electronic Health Records. Available at: https://www.ecri.org/components/HRC/Pages/MedRec1_1.aspx
- Guidance Article: Implementing Computerized Provider Order Entry. Available at: <https://www.ecri.org/components/HRC/Pages/Pharm6.aspx>
- Guidance Article: Medical Identify Theft. Available at: <https://www.ecri.org/components/HRC/Pages/SafSec12.aspx>
- Guidance Article: Patient Identification. Available at: <https://www.ecri.org/components/HRC/Pages/RiskQual16.aspx>
- Guidance Article: Patient Identification and Security Systems. Available at: <https://www.ecri.org/components/HRC/Pages/SafSec14.aspx>
- Patient Safety at Intersection of Medical and Information Technology. Available at: <https://www.ecri.org/components/PSOCore/Pages/PSONav0811.aspx>
- Risk Managers' 10 Strategies for Health IT Success. Available at: https://www.ecri.org/components/HRC/Pages/RMRep0613_Focus.aspx

* These items are available to the public for free.



Appendix B: Meeting Agenda

Partnering for Action: Applying What We've Learned

OCTOBER 16, 2015

Welcome and Overview

Ronni Solomon, JD, ECRI Institute
Jeffrey Lerner, PhD, ECRI Institute
Theodore Giovanis, FHFMA, MBA, JKTG

Moderator

Janet Marchibroda, MBA, Bipartisan Policy Center

Safe Practices Forum: *Partnership* Copy and Paste Initiative

Tejal Gandhi, MD, MPH, National Patient Safety Foundation

This session presents materials developed through the Copy and Paste Workgroup, including best practices, an evidence review, and Safe Practices toolkit. The *Partnership* will be asked to adopt the Safe Practices, and promote a campaign for disseminating the resources.

- **Multi-stakeholder Panel Discussion**

Lorraine Possanza, DPM, JD, MBE, ECRI Institute
Jeanie Scott, MT, (ASCP), CPHIMS, Veterans Health Administration
Trisha Flanagan, RN, MSN, athenahealth
Brian Crawford, Epic
Michael Victoroff, MD, Lynxcare

Safe Practices Forum: Patient Identification

This session launches a new *Partnership* workgroup on Patient Identification. Included is initial research on safety concerns associated with patient identification to begin framing the topic.

The discussion will focus on ways that health IT can make care safer as well as introduce unintended consequences. Audience perspectives will be sought.

- **Multi-stakeholder Panel Discussion**

William Marella, MBA, MMI, ECRI Institute
Jason Adelman, MD, MS, New York Presbyterian
Terhilda Garrido, MPH, ELP, Kaiser Permanente
Hardeep Singh, MD, MPH, VA Medical Center
Mark Segal, PhD, GE Healthcare
Lori Paine, RN, MS, DrPH(c), Johns Hopkins

Partnership Data Analysis (2015 report)

This session presents a summary of health IT safety events and hazards reported to the *Partnership*. All events will be non-identifiable.

Robert Giannini, BS, NHA, CHTS - IM/CP, ECRI Institute

DESIRED OUTCOMES

Make Healthcare Safer Together:

- Adopt the *Partnership's* Safe Practices for Copy and Paste.
- Establish communications for Safe Practices.
- Launch new Workgroup on Safe Practices for Patient Identification.
- Review the nature and type of safety events and hazards reported by the *Partnership*.
- Uncover challenges and barriers to health IT safety.
- Agree on which issues are of highest priority for follow-up.
- Inform the national strategy for health IT safety.



Breakout Sessions

Breakout sessions involve facilitated discussion on specific safety concerns identified in *Partnership* reports.

- **Shared Learning Forum: Hot Topics in Health IT Safety**
(Panel Discussion from Breakout Sessions)

Jesse Ehrenfeld, MD, MPH, Vanderbilt University and
American Medical Association

Dean Sittig, PhD, University of Texas

Kathy Kenyon, JD, Kenyon Law Firm

Feliciano Yu, Jr., MD, MSHI, MSPH, St. Louis Children's Hospital

Trish Lugtu, BS, CPHIMS, CHP, Constellation

Kalyan Pasupathy, PhD, Mayo Clinic

Christoph Lehmann, MD, Vanderbilt University

ONC's Health IT Safety Roadmap

Andrew Gettinger, MD, ONC

Next Steps and Adjourn

Janet Marchibroda, MBA

Ronni Solomon, JD



Appendix C: About our Speakers and Panelists

Jason Adelman, MD, MS, is the Chief Patient Safety Officer and Associate Chief Quality Officer of New York-Presbyterian Hospital/Columbia University Medical Center.

Brian Crawford is a leading member of Epic's patient safety and quality team, working to promote a strong patient safety culture focused on ease of reporting, urgent response, proactive communication, and continued improvement through root cause analysis.

Jesse M. Ehrenfeld, MD, MPH, is an associate professor of anesthesiology, surgery, biomedical informatics, and health policy at Vanderbilt University School of Medicine.

Trisha Flanagan, RN, MSN, is accountable for patient safety across athenahealth's cloud-based network including the electronic health record and the patient portal products.

Tejal Gandhi, MD, MPH, is President of the National Patient Safety Foundation and the Lucian Leape Institute. In this role, she is advocating patient safety at the national level, driving educational and certification efforts, and helping create and spread innovative new safety ideas.

Terhilda Garrido, MPH, ELP, is Vice President, HIT Transformation & Analytics in National Quality at Kaiser Permanente. She leads efforts and has published on Kaiser's work to understand, study, disseminate, and facilitate strategic value realization and patient safety opportunities.

Andrew Gettinger, MD, is the Chief Medical Information Officer (CMIO) at the Office of the National Coordinator of Health IT, professor of anesthesiology and adjunct professor of computer science, Dartmouth College & the Geisel School of Medicine at Dartmouth.

Robert C. Giannini, BS, NHA, CHTS – IM/CP, is a Patient Safety Analyst and Consultant at ECRI Institute. Giannini is a Certified Healthcare Technology Specialist (CHTS) as an implementation manager and clinician/practitioner consultant.

Theodore Giovanis, FHFMA, MBA, is the President and Founder of the Jayne Koskinas Ted Giovanis Foundation for Health and Policy and provides overall direction for the Foundation's activities.

Kathy Kenyon, JD, MA, is a former senior policy analyst of the Office of the National Coordinator for Health Information Technology. She remains active in the health IT arena.

Christoph Lehmann, MD, is Professor for Pediatrics and Biomedical Informatics at Vanderbilt University. He conceived and launched the journal *Applied Medical Informatics* and has served as the Editor-in-Chief since its inception.

Jeffrey C. Lerner, PhD, MA, MPhil, has served since 2001 as ECRI Institute's President and Chief Executive Officer. ECRI Institute (formerly the Emergency Care

Research Institute, founded in 1968) is the world's largest independent nonprofit health technology assessment organization that researches the best approaches to improving patient care.

Trish Lugtu, B.S., CPHIMS, CHP, is the Associate Director of Research at MMIC Insurance Inc., a Constellation company. Trish leads data analytics initiatives for medical professional liability claims to uncover patient safety learnings.

Janet Marchibroda, MBA, serves as the director of the Health Innovation Initiative and the executive director of the CEO Council on Health and Innovation at the Bipartisan Policy Center (BPC), following two years serving as the chair of BPC's Health IT Initiative.

William M. Marella, MBA, MMI, directs operations and analytics for ECRI Institute Patient Safety Organization (PSO) and the Pennsylvania Patient Safety Authority (PSA).

Lori Paine, RN, MS, is the Director of Patient Safety at the Johns Hopkins Medicine Armstrong Institute for Patient Safety and Quality and the Johns Hopkins Hospital.

Kalyan S. Pasupathy, PhD, is an Associate Professor of Health Care Systems Engineering in Mayo Clinic's Department of Health Sciences Research. He is the Scientific Director for the Clinical Engineering Learning Lab (CELL) within the Robert D.



and Patricia E. Kern Center for the Science of Health Care Delivery.

Lorraine Possanza, DPM, JD, MBE, is a Senior Patient Safety, Risk, and Quality Analyst and Health IT Patient Safety Liaison at ECRI Institute. She serves as the project manager for the *Partnership for Health IT Patient Safety*.

Jeanie Scott, MT, (ASCP), CPHIMS, is the Director, Informatics Patient Safety Program, Veterans Health Administration. She facilitated VA workgroup efforts to define and implement the VA's health IT patient safety program. She worked with the National Center for Patient Safety (NCPS) to develop key reporting, notification, and analysis processes.

Mark J. Segal, PhD, is Vice President of Government and Industry Affairs for GE Healthcare IT. Mark has been appointed to the National Quality Forum's (NQF's) HIT Patient Safety Expert Panel and is a member of the HL7 Advisory Council.

Hardeep Singh, MD, MPH, is Chief of the Health Policy, Quality & Informatics program at the VA Health Services Research Center for Innovations based at the Michael E. DeBakey VA Medical Center and Baylor College of Medicine, Houston.

Dean Sittig, PhD. Dr. Sittig's research interests center on the design, development, implementation, and evaluation of all aspects of clinical information systems. He is working to improve our understanding of both the factors that lead to success, as well as, the unintended consequences associated with computer-based clinical decision support and provider order entry systems.

Ronni Solomon, JD, serves as Executive Vice President and General Counsel for ECRI Institute, a nonprofit agency dedicated to promoting the highest standards of safety, quality, and cost-effectiveness in healthcare.

Michael S. Victoroff, MD, is President of Recall, Inc., a clinical informatics consulting firm. He is also the Risk Management Consultant for Health Information Technology at COPIC, Inc.; Chief Medical Officer at Lynx Collaborative Care Network; and Medical Advisor at Amara Healthcare Analytics.

Feliciano Buenviaje Yu, MD, joined St. Louis Children's Hospital as chief medical information officer and medical director of the Washington University Pediatric Computing Facility. He also was appointed an assistant professor of pediatrics at Washington University School of Medicine and maintains a clinical practice with the department of pediatrics' division of hospitalist medicine.



Sponsored by
 **JAYNE KOSKINAS
TED GIOVANIS** Foundation for
Health and Policy



PARTNERSHIP for
HEALTH IT PATIENT SAFETY
Making healthcare safer together

ECRIInstitute
The Discipline of Science. The Integrity of Independence.

For more information, contact hit@ecri.org