How to Identify and Address Unsafe Conditions Associated with Health IT Transcript

January 10, 2014

Presentation

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

...that's the basis of this webinar, but it has a policy context. So, next slide, important to understand. Can you put up the next slide? I'm not seeing the next slide.

[Slide: Policy Framework for Reporting to Promote Health IT Safety; 00:00:30]

The policy framework that supports this guide goes back to the Institute of Medicine report that ONC sponsored on Health IT and Patient Safety: "Building Safer Systems for Better Care." That report was finalized in November of 2011, and among other things it emphasized the importance of reporting health IT-associated hazards and events both by EHR users and by EHR technology developers.

Part of that was because the IOM felt that we needed more and better research to inform and prioritize health IT patient safety activities. So we need data to know what to work on first. ONC, based upon the IOM report, wrote a Health IT Patient Safety Action and Surveillance Plan that was published last July with the objectives of using health IT to make care safer. That's where I think we all are going. That is the hope for health IT. Part of that is to continuously improve the safety of health IT. Next slide.

[Slide: Reporting: ONC appreciates; 00:02:00]

We, in fact, learned a good bit since the IOM report and even since the Action and Surveillance Plan by the Department. One of the things I think we've known all along is that reporting of health IT-associated hazards and events is easier said than done. And indeed, reporting of adverse events in general on a voluntary basis is difficult. We know that there are low rates of voluntary reporting. Indeed, one of the promises of health IT is that it can make reporting itself easier. So, to improve reporting we know that it needs to be easier. Frontline clinicians and risk managers who are involved need to see a benefit. ONC has been talking to technology developers, the vendors, as well as developers of software applications who can help make the reporting of all adverse events and unsafe conditions but certainly those related to health IT easier using the Common Formats, the AHRQ Common Formats, which we will talk about more in this webinar. ONC obviously believes that patient safety organizations – and I hope you're all familiar with those. ECRI Institute patient safety organization is certainly one of the better-known ones, but there are many out there. We believe that they are a tremendous resource for EHR users as they move to reporting health IT-associated events.

As we've explored this area, however, we understand that there is a very basic problem in helping the clinical users on the frontline and the risk managers who often do the more in-depth analysis actually see the role of health IT in an adverse event or an unsafe condition so

that they can report it. That is in part the reason for this webinar. In our conversations and some of the research we've done, we know that what the clinicians on the front line and risk managers often see, they see the misdiagnosis. They see the wrong medication being given. They see a near miss that almost hurts a patient. They have more difficulty with the underlying role of health IT in the problem or in the solution. That's part of the reason for this webinar today.

I'll also note that ONC is working with others on this, including The Joint Commission, to provide education on the role of health IT in sentinel events. We're working with The Joint Commission on that. When you are doing a root cause analysis of an issue, of a sentinel event, you can recognize the role of health IT and we can learn from that. Next slide.

[Slide: Introduction of ECRI Institute speakers; 00:05:33]

Before I introduce the speakers, I want to note that this event and this guide is part of an ONC project that has been ongoing for four years on the unintended consequences of health IT. The contractor on that project is Westat, and they are the ones who are helping us with this webinar today. And I want to thank them for that.

But I also want to ask everyone to be on the lookout for a major project that ONC will be posting next week on it's called the SAFER Guides. The SAFER Guides are health IT safety self-assessment guides in nine areas which we know to be important, including the areas that we will talk about today in this webinar. And the SAFER Guides are major tools designed to help organizations optimize the safety and safe use of EHRs. So, please be on the lookout for that next week.

With that said, I am very pleased to introduce our speakers who are from ECRI Institute who wrote the underlining guide. ECRI Institute has been around for 45 years doing scientific research on a number of areas. ECRI Institute PSO has done research on health IT-related events in particular. From ECRI Institute we have Cindy Wallace, who's a Senior Risk Management Analyst, and Dr. Karen Zimmer, who's a practicing pediatrician and medical director for the ECRI Institute PSO and their patient safety risk and quality group. With that, I'd like to turn it over to Cindy.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Thank you, Kathy. And I'm going to put our slides up. Okay.

[Slide: Learning Objectives; 00:07:46]

Thank you, Kathy, and thank you to ONC for hosting this very timely webinar. As Kathy said, today we're going to talk about identifying and addressing unsafe conditions associated with health IT. And much of what we say today is summarized in the guide that was prepared for ONC entitled "How to Identify and Address Unsafe Conditions Associated with Health IT." The guide is publicly available. And if you scroll through, tab through your screen, you'll see a tab where you can access that guide. We'll also be putting the URL for the guide on the chat section in the right section of your screen.

[How to Identify and Address Unsafe Conditions Associated with Health IT Guide link: http://www.healthit.gov/sites/default/files/How_to_Identify_and_Address_Unsafe_Conditions_Associated_with_Health_IT.pdf]

The guide was prepared by ECRI Institute, which as Kathy described, is an independent nonprofit focused on identifying the best approaches to improving patient care. We manage several voluntary event reporting programs and altogether we've collected and analyzed more than 2 million patient safety reports. Some of those reports have been submitted to our federally certified PSO. In fact, some of the work that ECRI Institute PSO has done in analyzing health IT-related safety event is included in this guide and we'll be discussing during this webinar.

So, one other housekeeping detail, and I think a lot of you have already seen already, there's a Q&A feature on the screen. And we'll have time at the end of this webinar for questions. So please go ahead and submit your questions using that Q&A feature and we'll address the questions at the end of the prepared remarks.

So, let's start. We know that health IT can provide multiple benefits to patient care, but what happens when health IT operates in an unanticipated and unintended way? And how can health care organizations better identify these situations before they can lead to patient harm? Well, today we're going to try to answer those questions, and the learning objectives are listed on the screen. We're going to briefly describe the role of health IT in patient care. We're going to identify events that can occur when health IT operates in unanticipated ways. We'll look at some examples. We'll review a socio-technical model for evaluating health IT-related events. We're going to describe the high reliability and culture of safety principles for that reporting of errors, near misses, and unsafe conditions to be successful. We're going to then identify some tools and methodologies to assist health care organizations in developing reporting systems to capture health IT events. And finally, we're going to discuss some of the advantages for health care organizations to partner with their EHR developers and their PSOs in learning about and analyzing health IT events.

[Slide: What is Heath IT?; 00:11:05]

So, let's start with a common understanding about health IT systems. You see a definition on the slide that we'll be using. Health IT systems comprise the hardware and the software that are used to electronically create, maintain, analyze, store, and receive information in patient care. And this definition comes straight from the AHRQ Hospital Common Format that Kathy was talking about. There's a specific report form for health IT. And we'll be addressing these Common Formats later in the webinar.

[Slide: Examples of Health IT Systems; 00:11:40]

Now, for many organizations, health IT is synonymous with electronic health records, but we're looking at health IT to include other components that promote the exchange of health information in an electronic environment. So, some examples are listed on the slide. Administrative systems for billing and scheduling. Some technologies like automated dispensing cabinets for medication or certain computerized medical devices like infusion pumps with dose error reduction systems, what we often call smart pumps. Electronic health record systems and

their components such as barcoded medication administration systems and computerized provider order entry systems. Then there are also human interface devices, which is a fancy word for keyboards and monitors and touch screens. And then there are information systems from specific departments like laboratory, pharmacy, and radiology and diagnostic imaging.

[Slide: Health IT Can Enhance Care If… ; 00:12:50]

Now, as I've said, health IT can provide multiple benefits to enhance patient care, but it's like any three-legged stool, it has to be firmly supported by three essential elements. And in the case of health IT, they are, one, the technology has to be optimally designed by the system developer. Two, it has to be thoughtfully implemented by the health care organization. And three, it has to be appropriately used by the organization's staff.

So, Dr. Zimmer is now going to tell us a bit more about the benefits that health IT can bring to health care.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

[Slide: Benefits of Health IT; 00:13:32]

There are many benefits to health IT. And numerous studies support health IT's important role in patient safety. For one, with medication ordering computerized provider order entry systems, otherwise known as CPOE, can eliminate transcription errors for illegible handwriting. Health IT can provide clinical decision support to reduce medication errors. IT can alert clinicians to potentially dangerous orders such as patient allergy to a selected medication. Health IT systems can improve care coordination across setting by enhancing provider communication. It can provide clinicians with ready access to patient information to support treatment decisions in care planning.

[Slide: Unintended Consequences; 00:14:24]

But there can also be what we call unintended consequences of health IT when it operates in unintended and unanticipated ways. For example, the system might be unavailable for use. It could malfunction. The system could interact incorrectly with another, causing the data to become corrupted or the system could simply be used incorrectly.

[Slide: Examples of Unintended Consequences; 00:14:50]

Here are two real-world examples of incidents involving health IT systems that had unintended consequences for patient care. In the first example, the EHR developer notified its customers that a software prevented emergency physicians' medication notes from transferring to the enterprise medical record.

In the second example, a patient's blood transfusion was ordered and administered under her deceased husband's medical record. An alert nurse noticed that the patient's date of birth on her identification bracelet was not the same as the date of birth in the record that was pulled. Fortunately, the patient had the same blood type as her deceased husband. However, this error could have caused serious patient harm if the blood given to the patient was incompatible with her blood type.

Organizations must also be able to call upon their EHR developers for assistance in addressing unanticipated system faults. Like the EHR developer that discovered the problem with the ED module to its system, developers may also find that their systems function in unexpected ways in a health care environment, and they must be prepared to work with their customers to correct those bugs.

[Slide: Health IT Safety: A Shared Responsibility; 00:16:10]

But ultimately, a health care organization's approach to health IT safety really relies on the collective guidance provided by both internal and external experts as depicted in this slide. Working together, health care organizations, patient safety organizations or PSOs, EHR developers, and policymakers can learn how to achieve the full potential of health IT. For example, within the protected and confidential framework offered by PSOs, health care organizations can share with others their experiences with health IT systems to better understand problems and identify solutions. Additional guidance on health IT safety is available from federal and state health care safety authorities. This webinar sponsored by ONC is an example of such guidance.

[Slide: Socio-Technical Model for Health IT; 00:17:04]

Let's turn the program back to Cindy to start to look more closely at understanding the unintended consequences of health IT.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

So, as with many events involving medical technology, health IT-related incidents do not occur in isolation. The technology operates within a complex environment and health IT needs to be considered within the context of that environment. So, in trying to understand why a health IT event occurs, researchers have developed a socio-technical model for evaluating health IT within the context of eight dimensions. You see that model on the slide.

It illustrates a model that's been described by Dean Sittig and Hardeep Singh in their 2010 article in the Journal of Quality and Safety in Health Care. And the reference for that article is listed on the slide, although I think you might find it difficult to read, but there's also a slide at the end of this presentation on listing references, and you'll see this particular reference

there too.

[Slide: The Eight Dimensions of the Socio-Technical Model; 00:18:15]

So, let's look at these eight dimensions in more detail, and I'm going to linger on this particular side for a bit. So, the first dimension is hardware and software. That's the computers, the keyboards, the data storage, and software to run the health IT application. So, if an interface is not properly built between two health IT systems, problems can occur in the transfer of data. And we're going to look later at a specific example where lab results didn't get reported because of a poor interface between the lab system and another database.

The second dimension is clinical content. That's the data, the information, and the knowledge stored in the system. This might be, for example, the medications in the hospital formulary or a

default dose for a particular medication. And if not all the medications from the formulary are listed or if the default dose is incorrect, then medication errors can occur.

The third dimension is the human computer interface. That's the hardware and the software interfaces that allow users to interact with the system. How is the information displayed on the screen? If any information is cut off, the user may not see important information. For example, maybe if you can't see the full name of a medication on the screen and you need to scroll across or if important information about the patient is buried in a text note, there

can be problems.

The fourth dimension is people. That's your software developers, your IT personnel, your clinicians, health care staff, your patients, anyone who's been involved in health IT development, implementation, and use. And we all know that people can make mistakes in how the technology is used. Let's say there are two patients with the same last name on a care unit. How easy is it for a provider to pull up the wrong patient record of one of those patients with the same last name? Does the system have safeguards in place so that doesn't happen?

Now, the fifth dimension is workflow and communication. And these are the steps followed to ensure that patients receive the care they need at the time that they need it. How is the system used to notify a provider that critical test results have come back from the lab? Is there a process to ensure that the ordering provider or a designated backup is contacted within a specified timeframe if the results aren't reviewed? Otherwise, critical results

can be overlooked.

Our sixth dimension is internal organizational policies, procedures, the environment, and the culture. These are internal factors such as your capital budget, your policies, your event reporting systems, which can all affect aspects of the health IT development, implementation, and use.

Let's say that the organization has a policy to require barcode scanning of a patient's wristband to confirm the patient's identity, but if there aren't enough barcode scanners available because of limited resources, then staff may resort to workarounds, which can then lead to errors.

Our seventh dimension, the external rules, regulations, and pressures. These are external forces such as federal and state rules to ensure privacy and security protection or federal payment incentives to spur health IT adoption. And in the push to meet meaningful use requirements and to receive payment incentives for using EHR systems, is there a risk that the system isn't fully tested before it goes live and possibly glitches can occur that could interfere with

patient care?

And finally, our eighth dimension is system measurement and monitoring. These are the processes to measure and monitor the health IT features and functions. An example would be event reporting, what we're going to be discussing today. If the event reporting system isn't designed to capture information about health IT's role in the event, there's the risk that problems will go undetected and they can cause patient harm. So, when we examine health IT events, we need to understand them in the context of this model.

So, we're now going to look more closely at some of the most common problems that we've seen that can occur with health IT systems. And I'll let Dr. Zimmer discuss those.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

[Slide: Common Health IT Issues; 00:23:15]

At the most basic level there are two general areas. First problems occur at the interface between a computer user and the health IT system causing a person to use the system incorrectly. We call this a human computer interface issue.

Second, glitches can occur in how the equipment and software function. These are computer-related problems. For example, if software designed to connect one system to another has faulty coding, it could cause unexpected gaps in the transmitted data. Sample scenarios from each of these two categories, human computer interface and computer specific are listed on the slide.

As organizations try to understand why a particular problem arose with their health IT system, they can dissect these two general categories in greater detail. Did a problem at the human computer interface occur when data was entered into the health IT system or when it was retrieved? Did the problem arise because the computer user was interrupted or distracted from a task? For computer-specific issues, the organization can explore an array of questions that could have caused the incident. Was there a power interruption to the health care facility's computer network? Did information fail to display on the computer monitor? Was there a problem with the particular system's software, hardware, or both?

[Slide: Top Five Health IT-related Events; 00:24:45]

Using a taxonomy designed for in-depth analysis of health IT-related incidents, ECRI Institute PSO conducted an evaluation of health IT-related events and unsafe conditions to advance the understanding of technology and its impact on health care delivery. The taxonomy is described in a 2012 paper published by Magrabi and colleagues in the Journal of the American Medical Informatics Association. Again, the reference to that article is provided at the end of this presentation.

In its report "ECRI Institute PSO Deep Dive: Health Information Technology", the PSO shared information learned from the event. This included strategies to ensure health IT is appropriately implemented and used to improve health care quality without jeopardizing patient safety. ECRI Institute PSO's Deep Dive analysis evaluated more than 170 health IT-related events reported by 36 health care organizations over a nine-week period. The events ranged from data entries in the wrong patient records to gaps in reporting critical test results because the results could not be relayed electronically from one system to another. Some events involved more than one safety issue. This led to the analysis which identified 211 patient safety issues that were grouped into 22 event categories.

We'll summarize findings about the top five event categories identified in the report. Three of the five events fall into computer-related issues. They are system interface issues; software; issues related to the system's configuration; and lastly, software issues related to the system's

function. The remaining two are a human computer issue, specifically they are wrong data input and wrong record retrieval. These five event categories in total represented 64 percent of the 211 patient safety issues reported to ECRI Institute PSO.

[Slide: Case Studies: Computer-Related; 00:26:49]

Let's look at some examples from the report that fall under the general category of computer-related problem. System interface problems were the most commonly identified health IT concern in this analysis. These often resulted in missed orders for medications and various other types of tests. For example, a physician ordered a patient's anticoagulation medication to be discontinued. The order did not cross over to the pharmacy system and the patient received eight extra doses of the medication before it was discontinued.

A large percentage of the computer-related safety issues identified in the report were also associated with the configuration of a system's software. In one event a nurse tried to enter instructions and comments in the patient's record but the system prevented the nurse from typing more than five letters in the comment field.

In another example, the provider could not adjust a dose when utilizing barcode medication administration. For example, the automated dispensing machine only carries a particular dose of a medication, but when the dose needs to be split to provide the correct dose of a medication to the patient, what is the process?

Computer-related problems also occur when a health IT's system's software fails to function as intended. For example, consider when orders drop off an active work list. When an influenza vaccine was administered, it did not drop off after it was given. We have received reports where an error message was displayed each time a particular medication was ordered.

And lastly, there are a number of systems that do not alert when a pregnancy test is ordered for a male patient.

[Slide: Case Studies: Human-Computer Issues; 00:28:34]

So now let's focus on the human computer interface, two of the top-five HIT problem categories. Wrong data input was the most common problem in this category. And examples of such data included incorrect weight, drug allergies, or an identification number. And again, you can read the example on the slide.

What is most important to realize is that incorrect data entry errors are not unique to the EHR. They also occur with paper records. But in an electronic environment, the entry can automatically populate another field, multiplying the risks associated with the incorrect entry.

The second most common human computer issue is the wrong record retrieved by the computer user. In this case study the medication management system permitted the pharmacist to navigate off one patient profile and pull up another patient profile. As a result, an incorrect medication order was placed in the wrong patient's profile. The patient received incorrect medication. This scenario is all too familiar.

The last example shows how health IT risks may not be readily detectible. In this scenario a patient received a medication intended for another patient. The caregiver reporting the

incident categorized this event as a medication error, but the underlying cause of the incident was a suboptimal design in how the pharmacist interacted with the health IT system available.

To be able to make improvements to these systems, health care organizations must be alert to the possible role of health IT in an incident. I'll turn the program back to Cindy as we start to examine how health care organizations can better identify health IT-related incidents.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

[Slide: Identifying Health IT's Unintended Consequences; 00:30:23]

So, if health care organizations build this new foundation for care delivery with their health IT systems, they cannot presume that the systems will operate as planned or that patient safety is assured with the system. They have to operate as high-reliability organizations. And specifically what we mean by a high-reliability organization is one that makes safety its number one priority. It approaches safety systematically. So, try to picture the high-reliability organization as one that maintains a never-ending closed-loop approach to health IT system safety. That's depicted on the slide in front of you.

This approach entails continually monitoring for possible unintended consequences of health IT from the time the technology is first tested in the organization and throughout its full implementation and operation. And if any safety risks are identified, the organization must examine the causes of these risks using that socio-technical model that I described earlier and then consider strategies to eliminate the risk. And then it wants to select the strategies that work best for that organization in reducing risk and then monitor those strategies to ensure that they're working as intended.

And the goal for health care organizations is to design robust systems to capture the problems that users encounter so that they can be addressed before there's patient harm. In our closed-loop approach that's the section listed as identifying risks. So, in most health care organizations patient safety adverse event reporting systems provide a readily available process to identify risk. And these event reporting systems are primarily designed to keep patient safety, risk, and quality staff informed of incidents and near misses that affect patients. Traditionally they've been used to capture information about medication errors and delays in diagnosis, falls.

But most health care organizations' event reporting systems are not designed to capture information about the health IT's role in an event. We've been talking about those medication errors or delays in diagnosis where there could be a health IT aspect or a health IT has a role in contributing to that event. So, we'll get to how you design these systems to capture that information in just a bit.

But let's talk about the environment that's needed for effective reporting.

[Slide: High-Reliability Organizations' Commitment to Health IT Safety; 00:33:27]

For an organization's approach to health IT safety to be successful, the high-reliability organization that I was talking about needs to build a culture that supports staff reporting a problem that they encounter. The foundation for this culture is leadership commitment.

Leaders need to establish a safety culture. And many of you are aware of this concept of a safety culture, but it bears repeating that this applies to the health IT realm too. So, leaders show their commitment to educating staff about health IT safety, advocating that health IT is everyone's responsibility, promoting open communication about health IT safety concerns, and empowering staff to identify, report, and identify hazards and risks from their health

IT systems.

I want to just relate just a brief personal experience that I had with my laptop this week. I had a software upgrade installed on my laptop, and after the upgrade was installed, my internet function started to act up, and I was wondering is it just me or are others encountering this problem? Should I submit a help-desk ticket or not? And in a health care environment where patient care is involved, high-reliability health care organizations need to promote and empower staff that we don't want you to have to have this debate of should I or shouldn't I? We don't want staff to simply tolerate imperfection and glitches. We want to empower them to speak up when they encounter problems so they can address them before they lead

to any harm.

The leaders also need to allocate adequate resources to ensure health IT safety, both financial and staff. And most important, they need to establish a blame-free environment for robust reporting of health IT-related problems in an environment where staff don't fear punishment or reprisal.

[Slide: Event Reporting Within a Culture of Safety; 00:35:50]

To foster health IT event reporting, organizations must also educate their staff by providing examples of health IT-related incidents, examples like those that Dr. Zimmer has discussed. We want people to think outside of the box. We've been talking about the need to recognize that there may be more to a medication dosing error that deserves investigation. It may have an IT component or a delay in getting a critical test result may have an IT component.

Another point to emphasize with staff is that the organization is collecting information not just on computer-related failures like a screen display that's flickering but on the situations that make the health IT system difficult to use at the human-computer interface. This is often the information that doesn't get collected by event reporting systems. Information such it's difficult to find information from a pick list or the system requires that I make a hundred clicks through it to find that standard order set. Well, that might be an exaggeration, but having to click through various screens to get to information that you want can be a source of frustration and problems, and it can lead to potential problems with the patient care.

Organizations also need to educate their staff about how to submit event reports regarding health IT. And at the end of this PowerPoint presentation we've provided an appendix of slides that health care organizations can use to educate staff about reporting health IT events using the AHRQ Common Formats. And Dr. Zimmer is going to discuss how to use the Common Formats in just a few minutes.

Finally, staff need to know that their reports are acted upon. Their efforts of submitting reports should be acknowledged and staff should receive feedback about how the information was

used and whether it led to any changes. Within a safety culture these traits of acknowledging the reporter and providing feedback about reports are nearly just as important as establishing a blame-free environment. We often hear staff express frustration that their event reports go into a black hole and they don't know what happens to the information that they submit. So, by acknowledging and responding to these reports, staff are given the needed feedback that promotes continued reporting.

[Slide: How To Collect Health IT Event Data; 00:38:31]

Now, most event reporting systems are designed so staff can provide certain essential information about an event like the date, the time, the location of the event, and maybe a brief factual description of what happened. But how does this information help to convey information about the involvement of health IT? And unfortunately not all event reports are ideally structured for collecting information about health IT problems. The health care organization may need to reconfigure its event reporting system to collect information in a standardized format about the specific health IT issues involved. What system were you using at the time? What display were you looking at? What information was on the screen?

And fortunately there are resources available from AHRQ that can help an organization reconfigure its event report systems to collect health IT-specific data in both a standardized and a robust format. And these resources include the AHRQ Common Formats, which we've referred to already, and a prototype system called Hazard Manager. And Dr. Zimmer is going to describe these two resources.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

[Slide: How To Collect Health IT Event Data – AHRQ Common Formats for Health IT Event Data; 00:39:55]

So, AHRQ has developed event report forms that can collect health IT event data in a structured format to provide important information for meaningful analysis. These forms called the Common Formats for Event Reporting were developed by AHRQ to enable PSOs to collect all event data in the standardized format. The latest version of the hospital Common Formats includes health IT-specific questions to prompt staff to report pertinent health IT event data that will be helpful to the organization in reviewing and understanding the event in order to identify strategies to prevent the issue from reoccurring.

These questions have been incorporated into the form with the lengthy title "Device or Medical/Surgical Supply, Including Health Information Technology." The first page of the event report is shown on the slide, although I recognize it's difficult to read. So, like the other resources, you can download the form online, and this link is found in our guide. The form prompts the individual reporting the event to identify factors contributing to the incident, such as incompatibility between devices and an unexpected software design issue. Organizations may choose to supplement the data collected with an additional narrative field for those submitting incident reports to describe their concerns in detail.

[Slide: How To Collect Health IT Event Data – AHRQ Health IT Hazard Manager; 00:41:23]

To prevent further health IT errors, you need to really understand the entire life cycle of a health IT event, and that includes health IT hazards. While the common formats enable a computer user to indicate that health IT safety concern is related to the display of information on the computer, organizations may want to collect additional details about the concern to better identify corrective measures. The additional questions that you may find in the AHRQ Common Formats that could be helpful are what health IT system was used? What software version was used? Was a display screen used during the event? Who were the developers? And what was the event or the result? Was the result a user error, a health IT system error? Or a combination of both?

But really what you want to capture is information before it reaches the patient or better yet, before a system should go live. And you may want to identify such questions as was the information on the computer screen organized and clear? Was critical information available and observable? Was the text on the screen easily readable? Did the process charted by the health IT system match the users' workflow? Did the user interface reduce the short-term memory load? In other words, the user was not required to remember information from one screen when working in another screen.

Examples of these and other questions to consider are contained in AHRQ's "Health IT Hazard Manager," a prototype tool for health care organizations, EHR Developers, and researchers to report and systematically analyze health IT-related hazards and safety concerns. A snapshot of some of the information, as you can see, is on the slide, but again, difficult to read. So this resource is provided, a link in our guide.

At ECRI Institute we believe in order to make better sense of the data it is best to collect data with a standard taxonomy. So, in our PSO we utilize both of these taxonomies, AHRQ's Common Formats and Hazard Manager in one web-based reporting system.

[Slide: Health IT Event and Data Analysis – Case Study: Health IT Laboratory Event; 00:43:50]

Now let's look at a case study. Critical lab results were overlooked because of a poorly designed health IT system interface that hindered the reporting of critical laboratory results to a patient's physician. Here's what happened in this fatal event. The interface between a hospital's laboratory information system and its transplant surgery database only allowed certain laboratory test results to reach the transplant database. The transplant team had to access the laboratory system in the organization's EHR for additional test result information.

The transplant staff created a paper-based workaround. Using a printed list of transplant patients, the patient care coordinators would use the physician's password to enter his EHR inbox within the organization to find the laboratory results that could not be reported electronically to the transplant database. Once results were reviewed, the coordinator would sign off on the results, delete the notification from the physician's inbox, and enter an action item about the results in the transplant database.

When a particular transplant patient underwent laboratory testing, critical results indicating possible transplant rejection were reported to the laboratory information system but not to the transplant surgery database because of the incomplete interface between the two systems.

In this particular event the coordinator deleted the notification but did not enter an action item in the transplant database. Several months after the laboratory tests were conducted the patient died as a result of organ transplant rejection. Upon the patient's admission to the hospital for treatment for the failing transplant, staff discovered the original test result in the organization's EHR, which had indicated pending organ failure. The physician had never seen the test result to act on its findings.

[Slide: Health IT Event and Data Analysis – Case Study: Health IT Laboratory Event; 00:45:53]

Using the eight dimensions of a socio-technical model that Cindy described earlier, the organization can begin to conduct an in-depth examination of the event to understand how and why the health IT event occurred and ultimately to identify and design strategies to prevent similar events. Here's a partial look at what each dimension might reveal about the particular event.

Let's look at hardware and software. The system lacked an effective two-way interface between the lab and organ transplant program for ordering tests and receiving results. In terms of clinical content the test results were not stored in a structured format to facilitate reporting and tracking of the data.

Human-computer interface. Clinicians could not review test results in the patient's medical record and there were no alerts prompting clinicians to look for critical results.

People. The transplant staff created workarounds to an ineffective system interface.

Workflow and communication. There were no fail-safe measures to ensure that a clinician received critical test information.

Internal organizational policies, procedures, environment, and culture. The organization either failed to develop or enforce policies prohibiting the sharing of user passwords.

External rules, regulations, and pressures. Any number of external pressures, such as complying with federal meaningful use rules, preparing for an accreditation survey or handling unanticipated demand could have distracted staff and contributed to the event.

System measurement and monitoring. The organization failed to monitor laboratory test result follow-ups to determine whether critical results were received by clinicians for follow-up action.

The in-depth analysis of a health IT incident must be conducted by a multidisciplinary team of health IT system stakeholders as well those familiar with the particular hazard or incident. While organization event analyses have typically involved representatives from the clinical departments affected, incidents that involve health IT must include the IT department and other departments such as biomedical engineering familiar with the technology.

Just as James Reason's Swiss Cheese model for system failure illustrates that accidents are the result of multiple faults within a system that occur together in an unanticipated interaction, the socio-technical model illustrates the multiple facets within an organization that affect health IT safety. Cindy will address other aspects of the event analysis.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

[Slide: Monitoring and Staff Feedback; 00:48:41]

Okay. So, following this incident investigation or the event investigation, staff should be provided with feedback about the analysis, as I talked about already. And they need to know about the error prevention strategies that have been put in place so that they understand that their reporting leads to safer patient care and they continue to participate in the process.

Of course the organization must monitor the effectiveness of their new strategy and the solutions that they put in place to ensure that they're working as intended. And to reiterate, attention to health IT safety is a continuous process in the high-reliability organization. Remember that slide on the closed-loop approach.

Additionally, organizations must monitor the effectiveness of their event reporting programs to ensure that staff know how to use the program and that the program is capturing the necessary data for continuous improvement.

[Slide: Monitoring and Staff Feedback; 00:49:43]

But an organization's event reporting program should not be the only source for collecting data about the organization's health IT events. Throughout the health IT system life cycle it's important to talk to users and seek their feedback on the system's ease of use and determine what problems, if any, they're encountering. Senior leaders often conduct walk-arounds on patient care units. And that's an opportunity to ask staff about the health IT system, any problems that they're having.

Other information sources for potential health IT-related problems include help-desk logs that are maintained by the IT department. And we've heard of some health care organizations where the risk management departments are partnering with their IT department to be made aware of IT help-desk requests that have patient care implications.

There's also medical chart reviews. Such a review might identify, for example, frequent dosing errors for a particular anticoagulant. And again, maybe the default system in the electronic system was set incorrectly. Claims data is also important to look at. Are there certain trends that you're seeing in the data? For example, maybe there are claims that indicate that there are problems with delays in diagnosing patients' conditions in the ED. What's that all about? Is there a problem in how the test results are being electronically delivered to the ED providers?

So, we've described all these internal mechanisms for collecting information about health IT safety and now Dr. Zimmer is going to look at some of the external methods and describe how an organization might work with a patient safety organization and its EHR developers to improve health IT safety.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

[Slide: Reporting Health IT Events to Patient Safety Organizations; 00:51:47]

PSOs can serve as a source of external advice for health care providers seeking to improve the safety of health IT as well as patient safety more broadly. Federal laws provide that hospitals, doctors, nurses, and other health care providers my voluntarily report patient safety events to PSOs on a privileged and confidential basis for aggregation and analysis.

PSO activities are established under the Patient Safety and Quality Improvement Act of 2005, which creates a framework for health care providers to collect and share patient safety data in a non-threatening, confidential, and protected legal environment. Within this protected environment PSOs provide analysis and feedback about the events to help organizations make safety improvements, including health IT improvements.

Additionally, PSOs can collect the information in a standardized format using the common format to aggregate the data and identify trends that might not be detected beyond an organization's four walls and gain patient safety insights that can be shared with the health care community.

[Slide: Reporting Health IT Events to Patient Safety Organizations – workflow image; 00:52:57]

Based on the experience of ECRI Institute PSO and other collaborating PSOs, further learning may occur when multiple PSOs share aggregated data about health IT events reported to them. Because the common formats promote collection of this data in a standardized format, multiple PSOs can combine their health IT event data to spot trends, suggest health IT safety solutions, and ensure health IT is effectively used for patient care.

AHRQ has created a database called the National Patient Safety Database or NPSD, which can additionally analyze non-identified and aggregated patient safety event information that reporting institutions have agreed to submit. The database will only include the structured fields from the Common Formats and will exclude any free-text narrative entries. Nevertheless, these narratives have really important information, and that is why ECRI Institute PSO uses the data in its analysis and shared lessons learned.

The flow of the patient safety information from a health care provider to PSO at AHRQ's national database and back to the health care provider is depicted in this slide.

[Slide: EHR Developers' Role In Ensuring Patient Safety; 00:54:12]

EHR developers have a shared responsibility with health care facilities and health IT system users to ensure that technology is safe. The EHR developer code of conduct, which was issued by the Electronic Health Record Association, outlines EHR developers' patient safety responsibility. Any EHR developer that wishes to promote its adoption of the code must agree to adhere to the principles listed on the slide, but in particular, please note that participating with one or more PSOs and/or other recognized bodies for reporting, reviewing, and analyzing health IT-related patient safety events is one of the principles.

The EHRA's code of conduct reinforces what health care organizations should expect and demand from their EHR developers. As a customer, the organization should be able to contact the developer about a hardware and software problem to identify possible solutions to the issue. Similarly, health care organizations should expect and demand that their developer report known hazards and software bugs that could contribute to health IT safety events and to

offer solutions to the problem. There is a link for downloading the EHR developer code of conduct also found in our guide.

[Slide: EHR Developers' Role In Assuring Patient Safety; 00:55:31]

There are three ways in which EHR developers might work with providers and PSOs under the framework of the Patient Safety Act. They may serve as a contractor to a PSO. They may serve as a contractor to a provider or they may create a component organization to seek listing and serve as a PSO.

In the frequently asked questions about PSOs, AHRQ addresses these three ways in which EHR developers can work with providers and PSOs. And again, this link for the FAQ is also found in the guide.

[Slide: ECRI Institute PSO Pilot: Partnership for Promoting Health IT; 00:56:08]

I'd like to provide an example of how teaming up with a PSO can be valuable. PSOs create large volumes of data, and this data is afforded all the legal protections for patient safety work product under the Patient Safety Act. In an effort to reduce the health IT risks, promote patient safety and quality, and enhance health IT innovation, ECRI Institute PSO has initiated a multi-stakeholder collaborative which will bring together health IT developers, providers, and PSOs. This will be the first time vendors or health IT developers are working with patient safety organizations in this capacity.

The partnership will formally launch in 2014, and the data collection and analysis is projected to last for about a year. The partnership is using AHRQ Common Formats for health IT along with the HIT Hazard Manager to collect information on health IT events and hazards. The health IT developers, providers, and PSOs will collect the data. The review and analysis of the data will occur in conjunction with IT experts, human factor and implementation experts, and safety engineers and others.

The integration of reporting from various stages of events as well as from various stakeholders should yield robust lessons and improvements in the use and implementation of health IT.

[Slide: Conclusion; 0:57:08]

In summary, while we recognize the benefits of health IT, we also acknowledge that it can be associated with unintended error types, which if unaddressed, can lead to patient harm and undermine the goal to use health IT to improve patient care. Health care organizations should continually monitor and address health IT safety, but they cannot achieve the goal of health IT safety alone.

Providers, system developers, and policymakers must harness the information reported to external groups such as PSOs, which have the capability to identify trends and patterns from data submitted in a standardized format by multiple providers. Through this combination of a facility-level event monitoring and large-scale surveillance and analysis, we can foster the development, adoption, and use of the safest systems for the best care.

This concludes our presentation. Additional slides can be found for your reference, and these include important online resources that you can access from the guide, references to important

studies and publications related to health IT safety, and slides that organizations can use to educate your staff about reporting health IT events using the AHRQ Common Formats.

[Slide: Online Resources; 00:59:04]

[Slide: References; 00:59:05]

At this point I will now turn the presentation over to Kathy Kenyon.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

[Slide: Appendix: Examples of Health IT Events for Reporting into Device/Health IT AHRQ Common Format; 00:59:15]

Thank you so much for that wonderful presentation.

[Shared Document: How to Identify and Address Unsafe Conditions Associated with Health IT; 00:59:15]

I am looking at questions. A good many of them come from people who are basically addressing ONC and our rulemaking authority. And what I'll say is that none of the people on this call, including me, can really talk about that. In general, ONC has looked at safety-enhanced issues. What we might, you know, might have regulatory implications. That's why in stage two we have two certification criteria that were related to safety.

But in general, health IT safety initiatives have really had to grapple with the fact that you cannot get safety except by shared responsibility. You can have absolutely great technology and use it poorly and you can have technology that has some known flaws and use it safely and in fact improve safety with it. And so I think a lot of our efforts right now are really on the non-regulatory side to work with the people in the safety community, the patient safety community in general, and to ensure that health IT safety is part of that dialogue in that community.

So, that's – I'm not going to pick the specific questions on regulatory matters, although we got some great ones and I will make certain that the people within ONC for whom those might be relevant get those questions.

I have two questions that I think would be interesting from ECRI. The first is should an EHR have a screen readily available to report an event or near miss to make reporting events easy? And should an anonymous option be available? Another is has ECRI studied governance or data stewardship and how that impacts the people side of health IT safety? So, Karen and Cindy, I'll turn those over to you.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Okay. So, Karen, do you want to take the one about the screen?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

Should an EHR have a screen? I would agree that the easier you make reporting, the more accessible it is for an end-user to report an event, the more likely they would report a near miss or an event. As we commonly know, at least for an end user, we tend to self-correct. A lot of times we might open up a couple of charts and while we're entering, realize we're in the wrong chart and switch it ourselves. So, a lot of times we will notice things, and because we don't have an easy way to report an event or a near miss or even a suggestion to improve our workflow process, we tend to approach it individually and we correct it ourselves and then nobody hears about it.

So, having a forum where you can easily obtain that information is a super idea. But again, even if you do have a way to report that information, it would be very important for an institution to provide feedback because you don't want to fall into the tendency where people will report and then they hear nothing back.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

Should an anonymous option be offered?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

Absolutely. And actually it's interesting because in the AHRQ Common Format they do provide an anonymous option. So again, that's an excellent suggestion and I would actually suggest us continuing what AHRQ has already started in that form. But, yes, anonymous option should definitely be welcomed. Those are both excellent suggestions.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

And then the question: has ECRI Institute studied how governance or a data stewardship plan impacts the people's side of health IT safety? No, we haven't, but I think the question points to an important point, and that is that governance, your boards of directors, need to be aware of what's going on with the health IT system. They're the ones allocate the funds for these systems and will continue to allocate funds as organizations add to the systems, make improvements. So, it's really important to develop a set of metrics to monitor how the health IT system is working and make sure that your senior leaders and the members of your board of directors see these metrics on a regular basis.

There is a question and I know Kathy doesn't want to specifically address ONC's role, but there's a question about what role, if any, does the panel believe ONC should play in promoting the adoption of the NIST's usability protocols to prevent adverse incidents with the EHRs. We won't comment on ONC's role, but there's really an important hospital role here and we've advised that hospitals take a look at these usability protocols when they're planning their systems before they implement the systems. Look at these protocols because the usability is so

key to how the user – how that human-computer interface works. And health care organizations can use those protocols in deciding up front what it is they want that system to have.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

One of the questions that we are getting has to do with are there error prevention strategies and resources that are available? I want to once again encourage the people who are listening in to look next week when ONC publishes the SAFER guides, which are safety assurance factors for EHR resilience. And I think that that will be a major resource. But you do have things like the NIST guide currently available and of course ECRI and others have published that can be useful, some of which are in the list in this guide.

I think that we are really at the end of this webinar right now. Cindy and Karen, do you have one more question that you can see from the list we've gotten that you'd like to address?

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Yeah. I'm scrolling through and do the AHRQ Common Formats have an option to identify adverse events caused by copy/paste cloning or other productivity-enhancing features of EHRs?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

They do. For something very specific like that obviously you can free-text the stories surrounding it. They have the detailed questions of involving the – regarding the technology that's involved and where you think the mistake may – whether in this case it would be a combination, but because if someone's copying and pasting, you would want to investigate why they're doing that. So, really for the AHRQ Common Formats, if the structured fields don't have what you're looking for, they have the free-text fields where you can still share the examples of the type of mistakes you're seeing.

And, you know, recently there's just been a lot of press, as we all know, in the area of the concerns with copy and pasting and usability issues. And we're going to see more and more of this. And we really are at a crossroads where we really need to all be working together to have the technology enhancing our workflows. And we can't do that unless we're all working together.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

I see a question here on what stakeholders should be involved in events that have potential health IT implications. Any thoughts there?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

That's actually very important. A lot of times people will only involve the people immediately involved in the event. But you should involve the risk managers, your frontline staff, obviously the people involved in the event. But as I had mentioned earlier, you also want to involve people from your IT department, possibly biomedical engineering, as well as others. But again, what's really crucial is the importance of not just involving these people at the time of the event, but these people should be involved early in the planning stages. And we actually talk about a number of strategies regarding that in our Deep Dive. And so gathering the information of all these stakeholders and involving end-users and people from other departments early on, even in the purchasing stage, is really crucial.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Okay. There have been some questions on just the web address for accessing the guide, and you can go to www.healthit.gov where the guide has been posted and also in the slide presentation, the slide listed for resources. I'm trying to go back to that now.

[Slide: Online Resources; 01:10:18]

You'll see the URL to the guide right there in that slide.

[How to Identify and Address Unsafe Conditions Associated with Health IT Guide link: http://www.healthit.gov/sites/default/files/How_to_Identify_and_Address_Unsafe_Conditions_Associated_with_Health_IT.pdf]

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

Also in the chat box there's a link.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Okay. Great. All right. Here's a question. Can PSOs influence health IT system improvements given that these incidents occur within a complex environment outside of the PSO? I think you've kind of addressed that during the presentation.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

Yes, I would agree with that. You know, again, I think the advantage of being outside an institution is you're an objective observer. And just that ability to aggregate information from other resources, you're able to spot the trends that many people are unable to see, as I said, within your four walls. So, I do believe, and my colleagues at ECRI strongly feel that we really can make valuable improvements in this area and would really encourage people to look to external experts.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

There's a question that's come in that says what liability protections are available for people in organizations that report adverse events? They go on to say my understanding is that these are discoverable and that reporting them to a PSO is not necessarily a protection. Karen, I'm going to leave that one to you.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

What I'll say about that is facts are facts. So, when you report something into a system, whatever is in the actual medical chart is not protected. So, as I say, facts are facts. But your analysis, your interpretation is protected. So, if you write a free-text field of your understanding of how the situation occurred, that's protected because that's your opinion. That's your situation. But the facts of – a medical chart is not protected. So, there are a number of nuances to this. I'm sorry, what?

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

Yeah. Let's be clear that the Patient Safety Act does provide a federal legal protection for patient safety work product that involves reporting to a patient safety organization. It does not, as you say, include the things that routinely are part of the medical records of a health care organization. But for instance, Karen, if an organization collected information in an adverse event reporting system in the common format and submitted it with the intention of submitting it to a patient safety organization, that would be legally protected as I understand it.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

Correct.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Okay. Here's a question, an interesting question. Who in the health care organization is ultimately responsible for identifying, analyzing, mitigating, monitoring risks associated with health IT? Now, that's going to vary from one health care organization to another, but the premise of the question is certainly important, identifying someone who ultimately is responsible for coordinating this event reporting program. Typically in most health care organizations it's the risk management department that's responsible for that. But as I said during the presentation, ultimately everyone's responsible for reporting health IT events, but the question, I think, makes an important point that one department, an individual, an individual within that department, typically risk management, is responsible for the event reporting program.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

And I would like to echo that because ultimately it's everybody's responsibility. And one of the things that I'm seeing with the area of patient safety and quality is until everybody sees it as their responsibility, and it's integrated into their everyday workflow, we're going to still have problems. We can't keep having parallels, like a parallel path, that it's someone else's problem. It has to be part of everybody's problem. So, everybody should be identifying. Everybody should be working towards these mitigating strategies. But to Cindy's point, every facility has a different environment, a different culture, and different policies and procedures. And that really you need to leave up to the individual organization.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Here's a question. How will organizations have access to the national database to learn about health IT safety issues? Kathy, can you address that or Karen?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

For the National Patient Safety Database, well, to date my understanding is no one has reported into that yet. I know that is the goal of 2014 that we will be reporting into that. But ultimately, I can't provide the details on that.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

Yeah. We certainly have a national patient safety database that is set up. Right now most of the adverse event reporting is going to patient safety organizations. And there are some patient safety organizations that are doing analysis. The patient safety organizations are preparing to submit information to the network of patient safety databases. And so we expect that to be happening in the next year or so. But what that means – it doesn't mean that there isn't very useful aggregation and analysis of data that's happening right now. It's just that it's happening at the level of the patient safety organizations right now.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Kathy, there's another question that's come in, interesting question. To what extent is this reporting on risk management's radar screen? Are they working with their CIOs to assess the risk of IT infrastructure and changes to it? And I would say the risk managers I've talked to, absolutely this is on their radar screen, and they are looking at ways to modify their event reporting programs to collect that health IT information. Typically risk management and the IT departments haven't worked together, but they're finding that with the implementation of these EHR systems and the deployment of health IT systems that they really do need to build alliances with their IT departments. So, the answer to that question is yes, absolutely. It is on risk management's radar screen.

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

I was also going to say it reminds me of, you know, the patient safety and quality officers didn't historically necessarily work with risk managers and now it's very common that depending on the institutions, how you're structured, that those departments all work together or are even all combined depending again on your institutions. So, again, I feel like we now need to look at the IT departments and bring them in and see where do they now fit in with the patient safety, quality, and risk group.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Right. And absolutely when the event report investigation is going on, and you talked about this already, you need to bring your IT personnel into that event investigation to see if there was an IT component, and if there was, involving your IT department in finding the answer.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

One of the questions that we are getting is about how receptive the EHR developers, the vendors, have been in efforts to identify and remedy safety issues that are associated with their products. I think that this is an extremely important question. When we talk to the EHR developers, they are very deeply committed to safety. I think that what we are all struggling with is how do we put together a risk management structure, a patient safety structure that brings in everyone who needs to be involved to promote safety? Cindy was just talking about working with the IT department. Sometimes that IT department can't solve the problem without working with the EHR developers. And certainly in ambulatory practices, which often don't have much of an IT department, it is very important that we figure out how it is that you can have very good communication between the users of the EHR and the EHR developers. And that needs to be a two-way conversation. Both the EHR developers informing the EHR users of potential problems with their products and the use of their products.

One of the things I want to emphasize here is that very often, and this is reflected in the ECRI research, the EHR itself, the problem occurs not because there is something wrong with the EHR, it's because of how the EHR was implemented, how different components of an EHR interface, how it's configured. And sometimes it's very difficult to say whose fault it is. What we have to do is we have to get beyond trying to assign fault.

We need for EHR developers and vendors to come in and help with implementation and use issues, and we need for the EHR users to tell their vendors when it is that their products are just not easy enough to use and where they could make them better and safer. So, part of what we're trying to do here is encourage a dialogue that is part of a commitment to making certain that this powerful technology is used to make health care safer. And as long as people are blaming each other, it's very hard to have that conversation. Karen or Cindy, do you want to comment on the role of vendors further?

Karen Zimmer, MD, MPH, FAAP – Medical Director – ECRI Institute

Well, I was just going to elaborate that in that dialogue, the type of support will also vary from institution to institution. So, an ambulatory setting may need more support from an EHR developer, as you said, than maybe a larger institution that has a pretty robust internal IT department who can carry out an EHR developer's suggestions rather easily. So, unfortunately there is no one solution that will fit every organization, and that's why it's so crucial to understand the situation where the error occurred and to work within those parameters of each of those facilities and treat them individually.

Cynthia Wallace, CPHRM – Senior Risk Management Analyst – ECRI Institute

Kathy, I don't see any more questions in the chat so we'll turn it back to you.

Kathy Kenyon, JD – Senior Policy Analyst – Office of the National Coordinator for Health IT

We have gone until 2:30. I appreciate everyone who has stuck with us to the end. This was, I think, a very useful presentation. I want to thank ECRI Institute for its work in this area and Westat for facilitating the webinar. Thank everyone who attended. And please get in touch with ONC. My name is Kathy Kenyon. It's Kathy.kenyon@hhs.gov. Let me know what you think about this and what issues you see, and I will make certain that they go back to the health IT safety team here at ONC. Thank you very much.