MANAGING INFORMATION SECURITY

Maintaining Inpatient Privacy and Reducing Risk
MANAGING INFORMATION SECURITY | Maintaining Inpatient Privacy and Reducing Risk

EXECUTIVE DIALOGUE

Sponsored by Clearwater Compliance, LLC

2017

8 PANELISTS

MODERATOR

Suzanna Hoppszallern

CEO
Clearwater Compliance
NASHVILLE, TENN.

Suzanna Hoppszallern

SENIOR EDITOR
Hospitals & Health Networks
CHICAGO

Bob Chaput

CEO
Clearwater Compliance
NASHVILLE, TENN.

Debbi Muro

INTERIM CHIEF INFORMATION OFFICER
El Camino Hospital
MOUNTAIN VIEW, CALIF.

Erik Devine

CHIEF INFORMATION SECURITY OFFICER
Riverside Healthcare
KANKAKEE, ILL.

Derek Sailors

INFORMATION SYSTEMS DIRECTOR, INFORMATION SECURITY OFFICER
Community Hospital
MCCOOK, NEB.

Jim Hanson

INFORMATION SECURITY OFFICER
Avera Health
SIOUX FALLS, S.D.

Brenda Williams

VICE PRESIDENT, TECHNOLOGY SERVICES
Mosaic Life Care
ST. JOSEPH, MO.

Phil Miller

ASSISTANT VICE PRESIDENT AND CIO
Unity Health
SEARCY, ARK.

Lynn Witherspoon

SYSTEM VICE PRESIDENT, CHIEF MEDICAL INFORMATION OFFICER
Ochsner Health System
NEW ORLEANS

Hospitals & Health Networks
CHICAGO

Suzanna Hoppszallern

SENIOR EDITOR
Hospitals & Health Networks
CHICAGO
Developing a sustainable information risk management program is essential to the delivery of value-based care. Health care organizations are increasing safeguards on patient data and monitoring for malicious activities as the volume of valuable patient information grows and visibility of patient information across the care continuum increases.

AHA Health Forum convened a panel of information, technology and security executives July 28 at the American Hospital Association’s 2017 Leadership Summit in San Diego to examine how hospitals and health systems can develop sustainable information risk management programs. The panel explores the challenges and best practice solutions to ensuring compliance and the delivery of secured patient data.
MODERATOR (Suzanna Hoppszallern, Health Forum): What kinds of short-term and long-term measures are you taking to secure patient information in your organization?

LYNN WITHERSPOON (Ochsner Health System): Ochsner is in New Orleans and a Hurricane Katrina survivor. The day after the hurricane, we visited our outlying clinics to discover the state of our medical records. At that time, we had completed a lot of automation, but we still had legacy paper records, so those records were exposed ubiquitously around the system. The other challenge that we faced was that to access our electronic records, you had to be in our network. We had no provider portals and no way to access medical records from the outside world. On the patient side, it became obvious that many people needed access to information. They were scattered around the countryside and their 30-day supply of medications was expiring. We had to get patients and providers access to medication lists quickly. We learned a lesson about needing to make information available both on the provider side and the patient side. Over the next five or so years, our major projects involved opening access to the network – which creates another layer of concern around security and breaches.

Before Katrina, we really didn’t understand what we are beginning to understand today in terms of the vulnerability of electronic information. We focused on security and not access. So, the longer-term piece is that if information is going to flow with patients wherever they go, our security challenge now becomes more patient-centric and not so much provider-centric.

PHIL MILLER (Unity Health): In the short term, we’ve just been trying to accumulate resources to enhance our security. We’ve focused on education from the board room on down about the importance of managing information security. If we’re serious about making sure that we’re taking care of our patients, we have to do whatever it takes to mitigate against

“We’ve focused on education from the board room on down about the importance of managing information security.”
- Phil Miller, Unity Health
a potential security breach. We’ve been ramping up, adding resources, staff resources, system resources to be able to put us in the position we need to be.

BRENDA WILLIAMS (Mosaic Life Care): We are also continuing to provide education and the due diligence to ensure clinicians and others inside the organization keep our information safe. Our biggest risk is email solicitation of our caregivers and the potential of inadvertently opening malicious email. We have a sandbox that sits in front of incoming email and checks it out before letting any email into the organization, so it’s worth its weight in gold. We continue penetration testing, firewall monitoring and other due diligence. We are shoring up contracts to ensure vendors are doing their cybersecurity due diligence before we sign agreements.

DEREK SAILORS (Community Hospital): We’ve always had a technical administrative council that’s been supportive on new data center and cybersecurity initiatives, but now we’ve started reporting to our board on a quarterly basis with executive-level reports on firewalls, web filters, spam filters, and internal and external penetration testing. That’s really gotten them connected with us and that relationship allows us to do a lot of neat things.

JIM HANSON (Avera Health): We have about 40 hospitals and 200 clinics in five states. We are centralized from an information technology perspective, which helps with security. I’m in charge corporately of formalizing our vendor management program. We meet at least annually with our strategic vendors, talking with them about security – what are they seeing, what have they done in the last year, have they had an audit take place. If they’ve conducted an audit, we ask to see it. Our challenges first were with macros, then URLs, and lately we have had situations where somebody accessed a web mail and introduced a virus, so now we don’t allow web mail. We have about 40,000 end points on our network that we have to monitor, so a big challenge for us is on the biomedical device side.

DEBBI MURO (El Camino Hospital): We have learned a great deal. We thought our biggest risk was our employees, but we did a phishing campaign and our employees were actually very good at not clicking on the wrong links. So, while we’re training employees in security awareness, our biggest issue is our vendors. It’s important to do the business associate agreement work, but that still doesn’t necessarily protect you. You’ll have to work with your insurer to work through those challenges.

“We’ve come out with a guideline that a laptop is a privilege, not a right.”
- Debbi Muro, El Camino Hospital

Another focus for us is device asset management. We’ve come out with a guideline that a laptop is a privilege, not a right. We’ve put together a guidelines form that each employee has to sign. We’ve spent time just in the last couple of months remediating laptops, making sure they have patches and all the things that they need – but also making sure the person using that laptop is aware that they should not be storing it on the seat of the car.

ERIK DEVINE (Riverside Healthcare): We’ve installed application white listing across every end point. It was a challenge to get that going because it required a change in workflow. Every time we bring on anything new, it has to go through security first, which is in IT.

We’re really looking at our internal data, determining who has access to what type of data. We have file servers out there with thousands and thousands of files. If there’s an email in there containing protected health information, what if you get a phishing attack? We’re running a campaign to make sure PHI gets scrubbed from emails.

And we are looking at patient portals. I still think the community has not seen the importance of health
care information. I come from the finance sector and we worked hard to educate consumers about security. How do we educate the patient that this is just like online banking, but now it’s a medical record? How do we get them engaged, when they’re more worried about their credit cards. Paying attention to community awareness and training has always been number one on the list for us.

**BOB CHAPUT (Clearwater Compliance):** As we’re talking about all the end-point devices, the information’s more visible than ever before, it’s more voluminous and it’s more valuable. And because of all those factors, it’s more vulnerable than ever.

What we’re seeing lots of organizations do is absolutely deal with all the short-term items that you’ve all mentioned, but then they look ahead to where they’re going strategically. Because this is now affecting clinical work flows, administrative work flows; it’s not just about claims records anymore. And with biomedical devices, with the attack surfaces now potentially implanted in me or attached to me, it’s a whole new game.

Longer-term, we’re seeing adoption of the National Institute of Standards and Technology cybersecurity framework – a formal process outlined in its special publication 800-39, Managing Information Security Risk. And, we’re also seeing the adoption of a maturity model approach. In the old days, it was risk analyze the EHR. We’re way beyond that. It’s no longer once and done. Today it’s plan, do, check, act, plan, do, check, act.

**MODERATOR:** A number of you have mentioned regular reporting to administration. How are you keeping up to date and making sure that you have adequate resources?

**WILLIAMS:** We’ve had great support from our board on our compliance issues. We share our framework and we conduct regular assessments and share those results. As I mentioned earlier, we are focused on education. We work with our clinicians to ensure they know the right thing to do.

**SAILORS:** When the cybersecurity initiative started at our hospital, we didn’t have any cybersecurity specialists. We’re a town of 7,200 people in remote Nebraska. We sent all of our staff, including our clinical IT staff, to a cybersecurity foundations course. And then we targeted the key staff with certified hacker, certified cybersecurity architect and cybersecurity service provider training.

Once everyone was trained and aware, we then started attacking our users with internal phishing. We’ve actually phished our board. We go out
and drop USB drives in the parking lot and see if people bring them in. With all that, our leadership understands it. And that’s really what allows us to do what we do.

**HANSON:** We’re getting very good support from leadership, especially reporting-wise. As for a maturity model, we belong to a Catholic health care group of about 13 organizations that are working together to come up with a standard maturity model, whether it’s Baldrige or something else. We all approach it differently, but we’re trying to gain some consistency as far as maturity.

**DEVINE:** I’ve had no issues with budget. I have more of an issue with trying to get the projects done within the year timeframe that we establish, than getting more resources. And vendor management is a challenge; the vendor space is enormous. I get a call every week with someone new coming out with the best security feature ever. We also explore what we can do to support our vendors and neighboring hospitals, so we all have conversations about “what are you doing that makes it better?” I think a maturity model is hard to reach. Because there is no maturity model that will give you ROI when hackers are continually moving on to the next thing.

**MILLER:** Our board has wanted to know more, so I’ve been invited on a regular basis to meet with them. We’re trying to build that trust factor by putting the foundational things in place and then sharing with them how those things work. When we do phishing campaigns, why do we do phishing campaigns? What does that protect us against? How are we ensuring our staff is knowledgeable enough to know not to do these things because it makes us vulnerable? Trying to put it in terms that they can easily understand is challenging. But at the same time, they take that responsibility seriously and want to make sure we’re doing the things we need to do to protect our patients’ information.

**CHAPUT:** I think the agenda item is moving up into the executive team, into the board. A hospital CEO once said to me that taking care of patient information is as important as taking care of our patients. And a CIO from a large children’s hospital told me the last thing the organization wants parents to worry about is the safety of their child’s medical information.

And somebody mentioned the value insurers bring. They can have a meaningful conversation under the banner of executive risk, general liability and cyber liability. We’ve seen the executive risk broker be a very effective ally in this conversation.

**MODERATOR:** How are you addressing the challenges with clinicians in your organizations?

**WITHERSPOON:** The whole care paradigm is shifting from individuals coming into my office to suddenly I’m responsible for a population of patients
in the community. But our information infrastructures and security approaches are honed to deal with the past paradigms. I think it’s trying to imagine that future state and what those looming challenges will look like. Think about opening a whole bunch of application programming interfaces and all of a sudden you’re exposing an awful lot of data to the outside and trusting that whatever authentication strategy you’ve used is going to take care of that. We exchange about one million records a month using continuity of care documents. We have looming challenges that are different than what we’ve been thinking so far.

MURO: Another problem is having independent physicians on so many different EHRs, while you’re on a larger EHR, and you can’t achieve that interoperability yet.

MODERATOR: A number of you mentioned device control. What are the real risks?

MURO: Network segmentation is now not just a portion of the network, it’s partitioning based on application or device. We just built a parking garage with solar devices and cameras. All those end points can be used to come right into your network and take you down. I heard about a vending machine that had a credit card device on the network, and that was compromised and caused a denial of service issue. So, it’s not just biomedical devices, it’s every end point.

HANSON: Another aspect is vendor access. Giving them access to a device provides another access point we don’t control.

CHAPUT: A Target breach originated from an HVAC vendor having access.

WITHERSPOON: With the ubiquity of smart devices, it seems we’re running harder and faster, but falling farther behind. Looking to the community, and reducing the risk as opposed to trying just to lock everything down, seems what we need to be thinking harder about going forward.

CHAPUT: Yes, as information assets change from legacy systems to a wave of new devices, vulnerabilities are changing. We have to begin to project as best we can what the changing threat landscape is going to be. But we also must shift to more of a strategic, business-oriented view and a maturity model that at least provides a set of guiding principles.

MODERATOR: Do you have an information risk management program, and what lessons are you learning from it?

MILLER: Sure, we have been really trying over the last couple of years to formalize processes that in the past were a lot more informal. And in the future, I expect we’ll have an even more formalized process in place. There’s such a broad spectrum of possibilities that can impact us, so we have processes in place – from protection on the front end, with firewalls and antivirus and malware protection – to the back end, with infrastructure like disaster recovery plans.
**WILLIAMS:** As I said earlier, we’ve been doing annual risk assessments and penetration testing. In fact, I just signed a contract this morning to do a surprise attack on ourselves to see what happens. We have a retainer with a 24/7 monitoring partner, so they’ll help us with an incident if we should have one. We encrypt laptops, phones, every device we have, and so we’re safer when we do telemedicine. We have secure texting between providers and patients and the rest of the staff. And we continue to provide education to make sure patients on our portal know to be careful with their information.

**WITHERSPOON:** We have a formal NIST-based risk assessment and remediation approach. We’ve learned it’s important to focus on priorities and levels of risk because there are too many “rocks” and too much stuff under those rocks.

**DEVINE:** Risk management isn’t something you can check off and put away. You have to go back because a platform or product will have changed. One thing that’s come out of it is that before we sign a contract to buy a product, we know we have to be proactive and do the risk assessment, have IT sign off on it beforehand.

**SAILORS:** We do third-party assessments as well as our own security risk analysis, and do monthly briefings with the whole IT department. And we’ve been adopting the NIST framework. But starting out, we didn’t have any benchmarks. Now we establish those first so we can see what’s wrong.

> “Risk management isn’t something you can check off and put away.”
> - Erik Devine, Riverside Healthcare

**KEY FINDINGS**

1. **Education is important for counteracting the triggers often most responsible for opening the door to incidents:** employees clicking on malicious emails, clinicians bringing in their own devices, and patients not understanding that their health information is as at risk as their financial information.

2. **Many organizations are moving from reactive risk management to a more strategic, business-oriented stance, and adopting a risk maturity model approach and formal risk management processes such as the NIST cybersecurity framework.**

3. **A multitude of network end points, compounded by the growing use of biomedical and other devices, is making organizations more vulnerable to cyberattack. Network segregation and device asset management are two key ways to protect information.**
Clearwater Compliance, LLC
Clearwater Compliance, LLC is a leading provider of hospital and health system compliance and cybersecurity management solutions. Its mission is to empower hospitals and health systems to successfully manage healthcare’s evolving cybersecurity risks and ensure patient safety. Exclusively endorsed by the American Hospital Association, Clearwater solutions have been deployed within hundreds of hospitals and health systems, Fortune 100 organizations and federal government institutions.

LEARN MORE INFORMATION ABOUT CLEARWATER COMPLIANCE AT WWW.CLEARWATERCOMPLIANCE.COM