How Effectively Are We Protecting Protected Health Information?

Roundtable Participants

Joe Sheffer The loss of protected health information (PHI), including PHI stored on or transmitted by medical devices, is a major concern for healthcare delivery organizations (HDOs). How well is the industry safeguarding PHI, including deidentifying it adequately?

J.P. Larson One of the biggest challenges, for HDOs in general, is asset management. The repositories have not always been the best source of centralized information. We are methodically maturing our asset management capabilities by asking the right kind of questions and filling in updated information.

Another challenge is identifying and documenting what devices have PHI or even personally identifiable information (PII) because the manufacturer may support the storing of PHI but the organization may decide not to store PHI. For example, a device could have the capability of storing a sufficient number of identifiers—full name, date of birth, and gender—yet the practice might not use it in that capacity. In support of minimum necessary, the practice may just enter in one initial and the year. Therefore, organizations must identify and document whether the device really does contain PHI. Additionally, if the practice decides to change the way they enter data at any point in time, the Privacy Office, Clinical Engineering, and Information Security all have to be informed that the device will now be used to store PHI so that the classification for that device can change accordingly.

Axel Wirth The point J.P. is making is an excellent one. What we see is really a disconnect between systems and responsibilities. One party may need to go see somebody else to find a certain piece of information, yet it may not be that somebody else’s priority. I’ve seen those things happening all the time. On the system level, obviously, we have had asset management systems for a long time, but they are typically focused on the physical asset and on the traditional IT space. Taking a broader look, I want to include things like medical devices, billing systems, and systems in the parking garage that take photos of license plates.

It becomes a challenge for the asset management system to capture everything. That is a scope limitation. On top of that, even if an asset management system has captured an asset, it still doesn’t tell us whether that asset is an information risk and may contain PHI or other critical information because that was not the objective of the asset management system. So, whenever we get questions around PHI and PHI risk from a potential breach, what we find frequently is that that the systems that are implemented today are frankly challenged with answering those questions correctly.

Stephanie Domas I wanted to comment on a different facet of the question. From my perspective, I’ve seen a big increase in the use of strong encryption in medical devices when it concerns PHI, and that’s really great. But the problem we’re facing is that encryption only works if both sides support it—specifically with medical devices. I’ve seen both sides of the puzzle, where a hospital server may support encryption but the medical device does not, and I’ve seen medical devices that support encryption but are not configured to use it. The hospital never sets them up to use it.

So, while I have seen greater adoption of communication encryption in medical devices for protecting PHI, we still struggle with the need for encryption support from both sides—not just supporting encryption but supporting the same type and version of encryption, and then it needs to be set up correctly. That’s where I see the struggle right now in terms of protecting PHI.
Priyanka Upendra  From a technical perspective, I think we’re doing okay in this ecosystem. We do have new devices coming into the market that are being built with security in mind. But we have a whole lot of devices in production that don’t support encryption or will just crash if you load any kind of compensating controls. From an administrative perspective, HDOs are still lacking a lot of standard operating procedures and processes that can help us identify what kind of PHI or PII is stored or transmitted in these devices or how PHI or PII is being used. A standard process is needed for assessing the system’s clinical need and workflow, which necessitates whether you need to store or transmit PHI. HDOs need to get better with identifying and deidentifying the data.

David Finn  I’m a recovering chief information officer, and one of the things I see is the difference in the way we perceive PHI. As Axel touched on, historically in healthcare, we haven’t thought about data as the asset. From a clinical perspective, it’s just something you need to work with. You don’t really think of it as an asset that benefits your organization and benefits the care you’re providing the patient, so the IT perspective has been, “That’s not our data. We don’t use it, but we’ll try to store it for you and protect it as best we can.” And that means we keep backups.

From a clinical perspective, we haven’t ever historically had to think about where that data is located. Even from the clinical or IT perspective, we’re very good at finding data if we know it’s going to be there. Everyone knows there’s electronic PHI (ePHI) in the electronic health record (EHR), but it never goes missing from the EHR. It’s in the Word documents, spreadsheets, and emails, as well as the medical devices that no one has really thought contain ePHI. So, we have to shift our focus from thinking of data that is just there, when and where we need it, to thinking of it as an asset that needs to be protected, just like money in the vault—but in healthcare. It is the money in the vault; that’s how you run your business.

Joe Sheffer  What other types of data are at risk, and specifically, what other data may pose a safety risk and need to be protected?

Axel Wirth  Any data in safety-critical medical devices could become a risk, and that can be as simple as calibration data, safety limits. That’s non-PHI data, yet if that data get changed, that can have severe consequences for the patient. But even much more simple things like, for example, the device’s IP address and MAC address would allow somebody to spoof the device. Or, on the network level, alarms could get misrouted or delayed. There’s plenty of data that is directly or indirectly related to medical devices and their ability to function that can actually cause harm, yet it’s not PHI.

What we’ve seen in healthcare over the last decades is really that the Health Insurance Portability and Accountability Act (HIPAA) has driven a certain view of cybersecurity risk, and that view is very ePHI focused and, secondly, very confidentiality focused. Even though HIPAA includes requirements around availability and integrity, these have been less of a focus in the past because of the breach notification law. So, I think healthcare as an industry has blinders on in terms of PHI confidentiality as the one big problem to solve, while not thinking about non-PHI data or other data as critical for non–confidentiality-type problems.

David Finn  We’ve seen this transition over time, historically and partly because of HIPAA, where we were very focused on confidentiality. Then we saw a shift in what was happening in that data and in the kind of attacks on it and changes in the threat landscape, and it got very focused on availability. But, the bigger risk to that data, particularly ePHI in use in an HDO, may be the integrity—maybe you changed a dosage or a weight on a patient and all of a sudden what seems to be fine and protected and good data becomes life threatening to a patient. So, we’ve got to look at not only the confidentiality and the availability, but the caregivers also have to be able to get the
data. We have to have ways of knowing that that data is intact. Based on what they’re using it for, it must be high-integrity and accurate data.

Priyanka Upendra We’ve moved away from just focusing on data security to looking at safety of medical devices so we can provide reliable patient care. We store a lot of PHI in the medical devices and transmit that to the EHRs, allowing physicians to identify the patient and provide the right treatment. Apart from that, you also have a lot of diagnostic information that doesn’t necessarily include PHI or PII. That information is going to the EHR for the appropriate treatment plan.

That includes dosage information to ensure the right medication dose is delivered to the patient. If that was to be corrupted with, say, incorrect patient weight or the wrong type of drug, you have wrong medication being delivered to the patient. The same with availability: If you have an incident that’s impacting the hospital network, you are forcing your clinicians to work in a standalone mode, and most of them are not used to that.

So, there is a lot of havoc in the hospital. The same with confidentiality: Unauthorized access would allow the intruder to obtain the records of the diagnostic information or even alter or delete important medical information, which affects the safety and reliability of patient care.

Stephane Domas System configuration is one of those very benign pieces of data from a privacy standpoint, but one of the critical pieces of data from a clinical functionality standpoint. Consider something like the maximum joules that you should ever shock an adult patient with, there’s no privacy perspective from it. I don’t need to hide the fact that it’s typically 200 joules.

But if that configuration file in the software that’s checking that bound becomes manipulated, and there’s not appropriate hardware checks in place, suddenly you have a device that can deliver too high of a shock or even potentially too low of a shock to a patient who’s in need of defibrillation. HIPAA originally focused on confidentiality but evolved to now include availability and integrity. I really view this as a shift from an older, more innocent view of data. In the past, the concentration was much more about the protection of accidental disclosure. We really didn’t consider a lot of malicious intent. So that’s why confidentiality was so critical. And, over the last couple years, those rose-colored glasses have really come off. We’ve started to accept and embrace that there really is malicious intent out there, and protecting against that malicious intent is now what’s really driving the increased focus on integrity and availability.

J.P. Larson I like to take a technical approach on this as well. When I’m doing risk assessments for medical devices, I look at audit logs, diagnostic ports, and removable media. Many devices have the capability of exporting reports and DICOM images to removable media. Also, there are medical devices that have a diagnostic capability to which the manufacturing tech can connect to resolve issues. Often those diagnostic logs have a lot more information than they need to contain.

In addition, I have begun looking at the control boards of medical devices because I’m noticing that there are a lot of components such as storage devices on there that are not part of the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form or the technical documents. We would have no idea whether there is data being sent, possibly cleartext, to that storage device without visual inspections and vendor engagement.

Joe Sheffer Looking more closely at HIPAA Security Rule: Does it still make sense given the change in cyber risks?

Axel Wirth It’s time to take a serious look at the HIPAA Security Rule and reassess whether it not only fits today’s threats but also today’s IT infrastructure and the way data is being used, which is quite different. When the Security Rule initially was written, we didn’t have social media, we didn’t have personal smart devices, and we didn’t put data in the cloud. Those are all new technology inventions. And if you would take, for example, HIPAA, literally, it talks about data protection on removable storage media. Is the cloud considered under HIPAA removable
storage? Or is that something different? So, clearly, I think it is time to bring HIPAA up to 2019 and bring it into the future.

At the same time, we also need to take a step back and say, “Has HIPAA really helped security and healthcare? And what could be done better?” Because I think a lot of what we’ve seen over the past years, really in spite of HIPAA, shows us that that healthcare security is not improving. The number of breaches is still rising at about 10% per year. We’ve had events that have had huge impacts on care delivery, such as the WannaCry cyberattack on the U.K. National Health Service. We have had events that have actually impacted drug availability and the healthcare supply chain, such as Petya affecting Merck Pharmaceuticals. These events are much more complex and much more timely than what is actually covered under HIPAA today.

Priyanka Upendra When HIPAA came out, people knew about it, but nobody took real action until the HITECH (Health Information Technology for Economic and Clinical Health) Act became law, as it added a lot of teeth and fines if HIPAA rules weren’t met. Now we are in a place where the Food and Drug Administration’s (FDA’s) guidance documents are adding a lot of teeth and fines, but we really don’t have a mandate to follow specific recommendations listed in those guidance documents. So, a bit of work needs to be done in updating the standards that we have.

David Finn HIPAA was written in 1996, and the Security Rule became effective in 2005. Just by virtue of what has happened to care delivery models since 1996, what has happened to IT delivery models and IT itself since 1996 and even since 2005, it’s pretty clear that HIPAA is not going to support security in the world we live in today.

Additionally, it was written to be descriptive. It was not prescriptive, and it harkens back to Stephanie’s comment about a simpler, less complicated time. But, for instance, encryption under HIPAA is an addressable item. It’s not required. And if you’re sending data around the Internet today, it’s almost ridiculous to think you’re not going to encrypt it.

We have care delivery models and IT delivery models that are completely virtual and remote. How do you do that without things like two-factor authentication? We’re going to have to lay down some hard rules because we live in a very different world than the one in 1996. And some things are not going to be addressable. They’re going to have to be required, if everyone wants to play along this continuum of care and—even more importantly—the continuum of data.

Axel Wirth Even in the simpler world of 2005, did HIPAA actually work? Did it make healthcare a more secure place? If we look at the statistics, we see that it didn’t work. Therefore, it’s not just a question of updating the regulation but also updating the approach to how to regulate the industry to make it more secure.

David Finn It never worked because very few people actually implemented what was there. So there’s an enforcement component that we’re going to have to get back to at some point as well.

Stephane Domas From a medical device perspective, the technical safeguards under the Security Rule are really the ones that ring most relevant to medical devices. While I can’t point to any of them and say they’re not good security practices, they are harkening back to Axel’s point—they’re so generic, and it leaves a lot up to interpretation. Reiterating Axel’s example, a lot of them are dated in the sense of, “Where does cloud storage fall?” Because they’re so generic and left up to interpretation, you also get situations like we discussed where, for example, encryption is not used because the particular entity can show how their interpretation of the rules shows they do not need it. The technical safeguards under HIPAA aren’t bad practices, but they’re so generic and in some ways out of date when considering new technology.

J.P. Larson If we circle back to the reason why we’re all here, it’s that we’re trying to protect patients, whether they’re inside or outside of the hospital system. This goes above and beyond HIPAA, such that we need to be treating PII the same as PHI.”

—J.P. Larson, medical device cybersecurity specialist at Christiana Care in Newark, DE
need to be treating PII the same as PHI. Technology is always advancing and changing. We have wearable devices that can monitor health, integrations with Amazon Alexa and Google Voice, and a shift toward in-home monitoring as well. It’s very challenging to identify all these areas where we need to start protecting the patient.

Another point is that the HIPAA Security Rule requires risk analysis. It doesn’t make mention specifically of vulnerability scanning or penetration testing. While HDOs may be conducting vulnerability scans on a routine basis, if we really look at the technology behind vulnerability scanning, only security risks from layers 3 and up within the Open Systems Interconnection (OSI) model are being addressed.

Therefore, the threats and attacks that apply to layers 1 and 2—for example, cable cutting, wiretapping, MAC address spoofing, CAM table flooding, and VLAN hopping—are not typically reviewed as part of a risk assessment process for medical devices, but they are very real attacks that can be done. Granted, it might take a little bit more effort for someone to be physically within the network, but there could be lateral movement from a threat actor. Other techniques and tools for assessments beyond vulnerability scans are needed in order to provide a comprehensive risk picture.

Axel Wirth That's a very good observation, as these kind of attacks certainly have the potential to breach PHI. In addition, the threat potential is even more serious if you think about disruption. A layer 1 attack could be a physical attack, like something as simple as unplugging a device. A layer 2 attack could be hanging up network communication and disconnecting a device on the data link layer. Again, thinking about integrity and availability of devices, these considerations related to lower-layer risk considerations are certainly highly valid.

Joe Sheffer In October 2018, the FDA released draft guidance stating that "medical device security is a shared responsibility among stakeholders, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices." What are your thoughts on the agency’s recommendations?

Priyanka Upendra I was able to attend the FDA workshop in Baltimore with the American College of Clinical Engineering Task Force. Medical device cybersecurity is a shared responsibility among all the stakeholders in the medical device ecosystem. Although FDA’s approach and trying to help refine this ecosystem and the ability to assist HDOs and the HTM community is impressive, there are much broader concerns that are not outlined in the 2018 guidance document for premarket submissions for cybersecurity, more so because they're not mandated for the manufacturers or other stakeholders in this ecosystem. One of the main concerns was the discussion around the software bill of materials (sBOM). How will HDOs consume this information or will it be another document that we will go on collecting without knowing how to use or having the right resources for it?

A lot of discussion at the workshop was directed at medical device manufacturers rather than HDOs. We did see a few HDO participants. What we really need included in the guidance, or another document from the FDA, is how to make the best use of the information presented in the FDA guidance—sBOM, tiered risk categorization, and patch management. Let’s take a step back to the MDS² form. I don't think more than half of HDOs even have the skillset or resources to use information in the MDS² documents.

Related to tier categorization of risk, the FDA guidance document does not fully consider how all factors contributing to medical devices are used in the clinical setting. There should be some alignment with the categories of risk defined by the Centers for Medicare & Medicaid Services and The Joint Commission. If we can come to an agreement on a comprehensive definition of risk criticality that factors in the physical, functional environment, as well as cybersecurity risk, and develop a single approach to scoring, that will be a game changer. Right now, that comprehensive definition of risk is lacking.
The FDA guidance also mentions patch management and the potential of designing medical devices to auto-update patches. I don’t think that will be something that the manufacturers or even the HDOs will agree upon because you have a variety of devices that present different functions of different criticality and auto-updating is not feasible, especially if a critical device is being used and you don’t want an update to be pushed there.

A final point about the FDA guidance document is related to the CyberMed Safety (Expert) Analysis Board (CYMSAB), which was also talked about during the April 2018 medical device safety action plan. There was some confusion about what the CYMSAB will do. There was really no strong vision of what the CYMSAB activities will be, and if there is indefinite funding for its activities, and if there’s any overlap with what the Healthcare Information Sharing and Analysis Center (H-ISAC) or what a United States Computer Emergency Readiness Team (US-CERT) is already doing.

Another question that leaves us wondering about the CYMSAB is whether the research activities that are outlined regarding what the CYMSABs will do: Is that going to be funded indefinitely from the fiscal year 2019 digital health budget from President Trump? Will it be available free of cost to researchers with good intent or even to HDOs that are suffering because of resource issues when responding to breaches or incidents? So, these were just some of the thoughts I had on the 2018 guidance document on premarket submissions.

Stephane Domas In terms of sharing responsibility, the FDA guidance hits the nail on the head in that medical cybersecurity really can’t continue to progress without both sides of the fence working on it. I doubt that’s really a surprise to the industry. Whether you talk to medical device manufacturers or HDOs, most everyone is on board with this. They understand it’s a joint effort.

Where you have a lot of gray area and some clashing is regarding “whose responsibility is what.” For example, is a hospital responsible for setting up unique firewall rules for each medical device, or should each device come with its own firewall that’s already preconfigured? Priyanka mentioned software updating, and that’s another really big one where everyone on both sides of the fence agrees, “This is a shared responsibility. Patching software is important.”

However, when it comes down to the nitty-gritty, where is the actual line of responsibility? If a software or device manufacturer releases a patch, whose responsibility is it to get it to the medical device? Should the manufacturer be responsible for sending out technicians at their own cost? Is that a service agreement the hospital should have to pay for? Should the manufacturer push those updates over the air? Priyanka mentioned that over-the-air updates are probably not something hospitals would want. But if they can’t push it, is the hospital responsible for subscribing to email updates about alerts and then the manufacturer’s responsibility stops there?

I believe everyone on both sides agrees, “Yes, it’s a shared responsibility.” But there’s still a tremendous amount of gray area about whose responsibility is what? Where does that line in their responsibility lie?

Another facet is the liability side of things. Although everyone agrees security is a shared responsibility, who is held liable when something goes wrong? I’m not a lawyer and won’t pretend to be one, but I think product liability is going to play a part in cybersecurity when you start to get into situations where there was an update available but it hadn’t been applied. Then, if a cyber incident occurred, from a product liability standpoint, what’s a reasonable amount of time that the hospital should have had to apply the update? Or, should the manufacturer have done more to get the update out to the devices. Is it still the manufacturer’s fault because they posted an update but didn’t alert the hospital?

I’d love to never see a product liability case get into the court system with that scenario, but unfortunately, I think we will at some point.

David Finn I agree with Stephane: It’s going to take all of us, from the device makers, to the purchasers, to the security

“I believe everyone on both sides agrees, ‘Yes, it’s a shared responsibility.’ But there’s still a tremendous amount of gray area about whose responsibility is what? Where does that line in their responsibility lie?”
—Stephane Domas
people, to the clinical engineers. But as Stephanie touched on, the problem really is twofold. On one hand, we have a "starting-here-and-going-forward" problem: How do we improve the manufacturing, development, and deployment of new devices? In some ways, that's easier than what may be the bigger problem, which is going to take all of us, and that is addressing legacy devices. There are millions of them out there, and they may be 10, 15, 20 years old. And generally, the older the device, the more difficult it is to mitigate and manage. Like Stephane, I also hope the decision about who's responsible doesn't wind up being made in the courts. This is all the more reason for us to get together and try to solve this together now, before we have that issue.

Axel Wirth  Rounding off this topic—and we've already touched on it earlier—is that in addition to the disconnect in responsibility and disconnect in ownership, there's also a disconnect in regulatory objectives. Earlier we talked about HIPAA's focus being on PHI and FDA's focus being on regulating the device manufacturer and the actual safety of the device. If you take, for example, a digital X-ray system, the PHI on the system is regulated differently and it's the responsibility of the HDO, as compared with technical data on the device. Calibration, for instance, as safety-critical data, is regulated by the FDA and the manufacturer is responsible for protecting it. But, really, it's one device. It should have one holistic security posture. It should be covered under one risk analysis, yet we have multiple regulations that are coming together and create a bit of a disparate approach to what actually should be a holistic approach.

Joe Sheffer  What other government activities, if any, do you foresee changing the focus of healthcare and medical device cybersecurity?

Priyanka Upendra  I learned about the Health Industry Cybersecurity Practices (HICP) documents during the recent workshop. HICP is a four-volume series that talks about the best cybersecurity practices for HDOs of all sizes. The AAMI cybersecurity guide was released in May 2018, and the HICP document was released on December 28. Together, these make a great set for HDOs to read and implement from. The HICP documents are freely accessible.

Stephane Domas  An Internet of Things (IoT) cybersecurity law was signed into law in California. The main gist is that it's going to require, by 2020, manufacturers of IoT devices to show what are called "reasonable security features" on their devices. I'm very interested to see whether IoT cybersecurity bills are adopted in other states or even at the federal level.

For the most part, even though it doesn't necessarily require cybersecurity certifications, most of the rumblings I've heard about the California IoT law in particular is that a lot of device manufacturers interpret this as needing to get a cybersecurity certification or cybersecurity seal of approval on their devices. Although that's all well intentioned, I have seen from a number of industries, including the payment card industry, that compliance in these certifications doesn't always mean good cybersecurity. So, I'm curious to see where this goes.

I'm also cautious because I don't want cybersecurity related to medical devices to become a compliance game just to get a cybersecurity certification on your device. Although some certifications are very rigorous and strong, if the only goal is to be in compliance, there are often ways to do so without designing a good cybersecurity device. I'm curious to see how additional bills being ratified in other states might affect medical devices from a compliance or seal-of-approval game.

Joe Sheffer  Are there any other points we haven't mentioned or topic areas you'd like to amplify?

Axel Wirth  One area that unfortunately has not received enough attention is how to go about discussing cybersecurity in a meaningful way with nontechnical stakeholders, such as clinicians and patients. That is important for a number of reasons, obviously because their behavior impacts the
security of the device. If a physician uses a device in a very insecure manner, there needs to be some basic education on that.

However, it goes far beyond that. For example, with the recent pacemaker recall, FDA advised patients to talk to their cardiologists about whether the software upgrade was the right thing for them. At the same time, nobody had given the cardiologists the decision tools or the education they would need to answer that question.

Another important point is that we need to recognize that we are still "pre-event"—we have not heard of a cyber event that actually harmed a patient. How will the discussion on this topic change after an actual cyber event that results in patient harm, whether it’s related to an EHR or a medical device? The lack of participation of the patient and clinician communities will hurt us a lot at that point. I don’t think we should panic over it, but we should certainly take it seriously and proceed with a sense of urgency.

David Finn One thing in healthcare that we have to stop doing is thinking about whether something is a cyber risk, a security risk, an IT risk, or even a clinical engineering or medical device risk. These all are business risks for healthcare. Until the CEOs, CFOs, chief operating officers, chief medical officers, and chief nursing officers recognize that this isn’t about IT or devices, it’s about patient care and safety and clinical operations, we will not get the organizational focus we need.

I wish we could stop using terms such as "cyber risk" or "security risk." These are business risks, and that’s a shift in the way we think about the data and how we use it and how all these physical devices are actually being used. If you’re in the business of healthcare, you need to think of it in those terms.

J.P. Larson I couldn’t agree more with David. In the FDA guidance about shared responsibility among stakeholders, patients are among the stakeholders listed. But do we really foresee patients reading that FDA guidance? I am unsure whether patients fully understand the value of their medical records and what happens with them. There’s a stopping point: Patients understand the cost of their copay but not all the fees associated and all the parties that have legitimate access to their medical records. Something as simple as educating patients is very beneficial.

References

“One thing in healthcare that we have to stop doing is thinking about whether something is a cyber risk, a security risk, an IT risk, or even a clinical engineering or medical device risk. These all are business risks for healthcare.”

—David Finn, executive vice president of strategic innovation at CynergisTek in Austin, TX

AAMI Resources