PHI Hide and Seek

HIDDEN PHI CARRIES HIGH FINANCIAL RISK

By Ken Reiher, MBA



From left to right: Ken Reiher, MBA; Rich Temple; Jamie Pesci (Not pictured: Sarah Hodson Grady, CPHI, HCISPP, RYT-200)

BEFORE ELECTRONIC HEALTH records (EHRs) and digital technologies, patient information was stored on mainframe computers located in secure rooms or recorded on paper charts and kept in file folders. Shared access was limited. The monetary value of personal information was low, and so the risk of breach was low.

The technology storm of the past three decades has made access to electronic protected health information (ePHI) easier, which benefits patient care in an ever-fragmented delivery system, but is bad for information security. Protected health information (PHI) can be found in virtually every corner of a healthcare system, concealed in unlikely places. With each new technology, acquisition, or merger comes new vulnerabilities that may remain unseen until the right assessments are performed to uncover them.

I recently sat down with a panel of information and privacy experts from three healthcare organizations to understand their unique experiences with hidden PHI and how they've worked to mitigate the associated risks.

Reiher: ***In your experience, what are some areas where PHI can be hidden?***

Rich Temple, vice president, chief information officer, and HIPAA security officer at Deborah Heart and Lung Center in Browns Mills, NJ, focused on cardiac, pulmonary, and vascular care: There are many subtle places that can contain ePHI in a healthcare organization. Without proper monitoring, this poses a serious risk that could cause a breach with devastating consequences. For example, consider mobile phones still in use after a provider has left the organization. Though the provider has been disconnected from the hospital network, there may be circumstances where data that was downloaded up until the time of the disconnection could still be accessible. Even with the mandate that all emails containing PHI must be encrypted, there is still potential exposure here for PHI or, at the very least, sensitive business information being accessible on the device.

I also recommend paying close attention to a hospital's business associates (BAs). Though all BAs are required to sign a HIPAA business associate agreement (BAA), it is often very challenging for a hospital to ensure the BA maintains the highest security possible for its data. There have been many documented cases[1] of BAs inadvertently publishing PHI. Often, it is just a simple misconfiguration on the part of the BA, but the hospital is ultimately liable for the mistakes of its BAs.

Yet another area that needs to be monitored is PHI downloaded by individuals or physicians via remote connection to the hospital's system from a home computer. Strict policies should be employed to ensure this cannot happen. Once PHI is on a personal home computer, it is highly probable that strong security safeguards, including encryption, are not present to protect that sensitive PHI from unauthorized access.

Sarah Hodson Grady, CPHI, HCISPP, RYT-200, conversion project manager/HIPAA security at Logansport Memorial Hospital, a not-for-profit medical center serving north central Indiana: Some EHR systems use Microsoft products that allow physicians to compose letters to, or on behalf of, patients. Though the EHR may launch, store, and save the file appropriately, this does not prevent a provider from storing that file elsewhere, such as on a local device. No EHR demo would reveal this behavior, but it does happen, and it's a great example of hidden PHI. Physician devices need to be audited frequently to discover such issues.

Medical devices are another place where patient identifiers could be readily available. It is important to ensure that patient identifiers are removed from the device. I recommend a standard process to promptly transfer the information from the record to the patient's chart and remove it from the device. This eliminates the possibility of filing a breach on anyone who might have been on that machine.

Jamie Pesci, director of health information management (HIM) and privacy officer for Christian Health Care Center, a nonprofit, healthcare organization offering senior living, short-

Top 10 PHI Vulnerability Assessment Questions

TO HELP UNCOVER hidden PHI, the following questions are recommended:
Does your organization:

1. Have a policy and process to lock down user workstations based on an analysis of risk and operational need?
2. Encrypt ePHI on portable devices such as laptops, tablets, USB/flash drives, external hard drives, and other electronic equipment?
3. Know which controls are in place to protect ePHI that is stored in remotely hosted databases?
4. Secure/encrypt the wireless transmission of ePHI within your facility?
5. Encrypt remote access transmission of ePHI?
6. Have policies and procedures in place for secure, complete destruction of any hard drive that contains ePHI?
7. Receive a certificate of destruction if using an external resource for disposal?
8. Have physical and technical safeguards in place for the patient portal?
9. Have a BAA in place with any telehealth vendors?
10. Have cybersecurity technology and processes in place to secure your internal network from intrusion?

term rehabilitation, and mental health services: ePHI can lurk in a variety of places, including hard drives and mobile devices of employees who work from home, and with business associates or their downstream third-party vendors. Pay attention as well to disgruntled employees who could be a source of breach if they have access to ePHI and a motive to share it inappropriately.

Reiher: ***Describe the potential risks—financial, operational, and reputational—of not uncovering these types of PHI locations.***

Temple: In 2018, the Ponemon Institute reported[2] that the average cost of a data breach in a healthcare organization is $408 per record, with an aggregate total estimate of breach costs at $3.6 million. So there is a devastating out-of-pocket expense for a healthcare institution in the form of fines, credit monitoring, and other expenses. That doesn't even include the loss of goodwill and trust in the community where the hospital operates. The reputational loss is incalculable in dollars and cents. Trust, once lost, is very hard to regain.

Grady: Failure to turn over every rock is like agreeing to babysit without knowing how many kids are in the house. A large breach could mean a loss of independence or autonomy, even if it does not take a healthcare organization completely under.

In a recent case, Hancock Health in Indiana[3] managed to protect its branding following a ransomware attack by hackers who accessed the hospital's data via a third-party vendor's remote connection. Hancock paid the $47,000 ransom and was able to retrieve patient data. The situation was not enviable, but the approach is definitely worth considering.

Pesci: The risk is huge to our reputation as a valued healthcare provider, jeopardizing our commitment to those entrusted to our care, the community, and our mission.

Reiher: ***What role does HIM play in data privacy at your organization? Are they part of a broader governance and advisory group?***

Temple: In our organization, HIM plays a leading role in data privacy. They spearhead our compliance with data retention requirements, and are closely involved with our committees that oversee privacy and security. HIM works with both our compliance department (privacy) and with our information systems (IS) department (security). HIM professionals are critical and knowledgeable partners in both realms.

Grady: Our privacy officer works directly with HIM to elevate data privacy issues to our governance committee.

Pesci: HIM plays a huge role in privacy for our organization. The director of HIM serves as the privacy officer who creates policies, monitors regulations, reviews subpoenas and court orders, controls access to records, and participates in performing risk assessments. We have implemented BA accountability, requiring the completion of a questionnaire regarding HIPAA compliance programs. We then assign risk.

The privacy officer, in coordination with the security officer, conducts HIPAA rounds. The privacy officer also serves on the corporate compliance team, monitors potential breaches, and educates employees, volunteers, and vendors using a variety of tools. In addition, the privacy officer maintains, updates, and posts the notice of privacy practices. HIM is the hub of the release of information.

Reiher: ***Describe a success story in which your organization was able to uncover hidden PHI and mitigate risk.***

Temple: We have a strict policy in place with employees who are granted access to our email server through their mobile devices. When they terminate employment with our organization,

Continued on page 55

Continued from page 26 ("PHI Hide and Seek")

they need to visit the inormation systems (IS) department—or have the IS department visit them if the termination is abrupt—to have access to our email server manually removed from their phones. We inventory and document all the mobile devices that are receiving email. And as part of our bring-your-own-device policy, we have the right to wipe an employee's entire phone if they don't allow us to remove their hospital access. So far, we have not had to wipe an individual's phone involuntarily. However, their awareness of our right to do so ensures compliance with our mandate and assures confidence that we have removed all PHI that we possibly can.

Grady: Every time you repair a hole in the dam, you find three new leaks. That is the nature information security in healthcare. Through rapid adoption, IS evolved too quickly as organizations were eager to take advantage of it. As a result, it's difficult to mitigate risk 100 percent. What we can do is exercise diligence regarding vulnerability assessments and make sure we fill any identified gaps.

Pesci: About 400 decommissioned workstation hard drives were being stored in one of our storage areas. We weren't certain about the level of data on them, but we discovered that some had PHI information. Therefore, we engaged a HIPAA-compliant recycling company to properly dispose of them, providing documentation of proof of destruction and recycling.

Hidden PHI can expose any healthcare organization to extraordinary risk, regardless of the provider's size, location, or complexity. Look under every rock, in every corner, and any other place where PHI might reside. The panelists shared examples, such as a storage room with decommissioned equipment—an area that could easily be overlooked. But these vulnerabilities can be found and addressed with the right assessment and mitigation processes. O

Notes

1. Healthcare IT News. "The biggest healthcare data breaches of 2018 (so far)." https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.
2. IBM Security. "2018 Cost of a Data Breach Study by Ponemon." https://www.ibm.com/security/data-breach.
3. Davis, Jessica. "Hancock Health pays $47,000 ransom to unlock patient data." *Healthcare IT News.* January 16, 2018. https://www.healthcareitnews.com/news/hancock-health-pays-47000-ransom-unlock-patient-data.

Ken Reiher (ken.j.reiher@complyassistant.com) is vice president of operations at ComplyAssistant.

Continued from page 39 ("The Danger of Being Connected")

The HHS voluntary guidance publication, described in the preceding list in item five, identifies medical devices as one of the top five cybersecurity threats to the healthcare industry. Offering practical solutions for small, medium, and large organizations, the guidance can be downloaded from the Public Health Emergency website.

Fortunately, within the last year, solutions designed specifically for medical and IoT device security have appeared on the market. These systems leverage automated and intuitive technology to passively scan the network without disrupting the devices or network activity, then parse the network metadata to automatically classify, manage, and safeguard all the devices.

This new visibility into device inventory and communications promises health systems the ability to apply sophisticated machine learning to accurately classify each device and leverage artificial intelligence to baseline its dynamic behavior within the context of a provider network. This additional level of detail should permit clinical engineers and chief information security officers to engage the IT department in defining and implementing actionable policies that significantly reduce exposure to patient harm and regulatory noncompliance.

Healthcare organizations like CHIME and AEHIS have discovered that patient safety risks attributed to medical devices are not contained to the device itself. These risks extend to the network, firewalls, switches, and operating systems. Healthcare delivery organizations are recognizing that medical, IoT, and OT device privacy and security are components of enterprise cyber and privacy risk management. A holistic approach is the only reliable way to deliver closed-loop security for patient safety and critical assets in our hyper-connected healthcare enterprise. O

Notes

1. Ponemon Institute. "Medical Device Security: An Industry Under Attack and Unprepared to Defend." https://www.synopsys.com/software-integrity/resources/analyst-reports/medical-device-security-report.html.
2. Kerravala, Zeus. "IoT Security Plans: 3 Things You Must Include." *Network World*, February 27, 2010. https://www.networkworld.com/article/3343184/protecting-the-iot-3-things-you-must-include-in-an-iot-security-plan.html.
3. Roberts, Paul. "What's the Value of a Stolen Chest X-Ray? More Than You'd Think." *Data Insider*. January 26, 2017. https://digitalguardian.com/blog/whats-value-stolen-chest-x-ray-more-youd-think.
4. The College of Health Information Management Executives and the Association for Executives in Healthcare Information Security letter to Sen. Mark Warner, March 22, 2019. https://chimecentral.org/wp-content/uploads/2019/03/CHIME-AEHIS-Warner-Response-vFINAL.pdf.

Ty Greenhalgh (Ty@CyberTygr.com) is the managing principal and founder of Cyber Tygr.