COSMOS
Navigate the Compliance Universe

Compliance Today - October 2019
Privacy compliance concerns: Privacy and security risk assessments of healthcare institutions

By Amit Sarkar

Amit Sarkar (amit.sarkar@eyecareleaders.com and amit1.sarkar@gmail.com) is Vice President, IT PMO and Governance at Eye Care Leaders in Charlotte, NC.

When an unnamed woman filed a complaint in the US District Court in Kansas[1] on May 11, 2019, against Atchison Hospital stating that the hospital had shared her individually identifiable health information (IIHI) with her rapist, it underlined a major Health Insurance Portability and Accountability Act (HIPAA) violation arising from badly formed and poorly executed privacy policies. The complainant further stated that, after the rapist was tipped off that she had named him as the rapist, he proceeded to harass her online, on social media, through text messages, and through phone calls before sexually assaulting her a second time. This unauthorized access and disclosure might have affected only one person, but the severity of the personal harm, which includes a second rape, should have brought the hospital under the radar of the HHS Office for Civil Rights[2] (OCR) and Office of the Inspector General (OIG).[3]

What can be done?

To prevent a similar incident in your healthcare facility, several proactive steps must be taken.

Restrict access to PHI and ePHI

The complaint referred to a letter written to the woman by the hospital CEO John Jacobson in November 2017 that affirms the fact that a former X-ray technician at Atchison Hospital had wrongfully accessed the victim's IIHI to tip off the rapist. Moral issues aside, it reflects poorly on the hospital's policies and procedures that a lab technician, who was in no way involved in the victim's treatment and rehabilitation, could easily access any patient's protected health information (PHI). As a punitive measure, the hospital terminated the X-ray tech's service, but the damage had been done.

Enforce tighter access controls and audits: This case underscores the dangers emanating from privilege misuse. Tighter access controls and audits followed with regular trainings would have prevented not just the breach, but also the tragic consequences for the victim.

Understand your risk position and the threat landscape

Don't become another statistic of the annual breach roster. With hackers getting savvier, the number of breaches and people affected by compromised data is sadly on the rise. The healthcare industry is one of the lowest performing industries in terms of endpoint security, posing a threat to patient data and potential patient lives, according to Beazley Breach Response,[4] a breach response management and information security insurance solutions provider. The earlier a breach is identified, contained, and reported, and mitigation actions are put in place, the lower will be the cost to your organization—both in a monetary sense and in terms of reputational loss. Every healthcare institution must periodically carry out risk assessments to identify vulnerabilities. Still,

you should watch out for these issues.

IT issues that hit clinical practices, behavioral health organizations, long-term care facilities (LTCs), and home health agencies (HHAs) include poor patching patterns, such as ignoring security updates periodically released by software companies; unsecured emails that allow phishing attacks to go unnoticed until even the servers are compromised; inadequate training; and targeted ransomware attacks. Remember, even if none of your own computers or Internet of Things (IoT) devices used by any of your personnel are affected, the ePHI of your patients could be compromised because of a breach occurring at your billing provider or at a pharmacy.

Take the case of OS Inc., a billing vendor, usually considered a premier partner in revenue cycle management services. On May 2, 2019, OS began notifying providers[5] at Sauk Prairie Healthcare, Tahoe Forest Health District, Sparta Community Hospital, Spectrum Health Lakeland,[6] and the Idaho Department of Health and Welfare that the ePHI of their patients may have been compromised, at least partially thanks to a hacking carried out through an employee's email account. The employee had fallen for a phishing attack, and the hacker had gained the employee's credentials in October 2018, two months before the breach was uncovered. This reinforces the Verizon finding that 93% of malware come from emails.[7]

Notify the affected parties promptly: Note that OS violated the provisions of the HIPAA Breach Notification Rule,[8] because any breach must be reported within 60 days of discovery. They waited for the conclusion of the investigation before beginning to notify the affected providers. Sensitive information breached included insurance numbers/Social Security numbers, dates of hospital encounters, demographic details, patient names, and account balances.

Patch vulnerabilities to save a great deal of heartburn

Regular scanning of systems is critical to identify vulnerabilities. This includes checking for flaws in software that could act as attack magnets and requiring remedial actions. If your institution uses a cloud-based email service, you should carry out a business associate agreement (BAA) with your provider to affix responsibility and liability, if a breach hits you. If you wait for a breach to hit before awakening to jeopardies, your organization is headed for a disaster.

Follow basic hygiene: "Most data breaches occur because of a failure to patch, yet many organizations struggle with the basic hygiene of patching," ServiceNow Security and Risk Vice President and General Manager Sean Convery was quoted in the Ponemon survey as saying, "Attackers are armed with the most innovative technologies, and security teams will remain at a disadvantage if they don't change their approach."[9]

Regularly update software patches: Out-of-date operating systems invite malware and hackers. Security experts pointed out in a post about the WannaCry attacks in May 2017 that out-of-date operating systems make any computer or smart device a sitting duck for privacy breaches. Ensure your IT team is diligent about updating all devices in your organization at regular intervals. Especially, all computers and laptops that are served by the organization's LAN or WAN and are interconnected should have their operating systems and other security measures, such as firewalls, updated to prevent breaches.

Heed the warnings: Negligence could sink you. Part of the negligence from healthcare organizations (e.g., hospitals, LTC institutions, skilled nursing facilities, behavioral clinics, medical practices, home health agencies), and whoever else might be affected by a data breach, emanates from a perception that it won't be them. The healthcare industry is especially unlikely to perceive threats to their data. The OCR repeatedly reminds people to implement proper mechanisms for safeguarding ePHI as required by the HIPAA Security Rule—a warning which is ignored all too often.

Address potential vulnerabilities to preserve confidentiality

Your security management should institute policies and procedures to govern the receipt and removal of laptops that contain ePHI in its facilities. In case of the Feinstein Institutes for Medical Research, Manhasset, New York, it was an unsecured laptop of a business associate, stolen from an employee's car, that got them slammed with a whopping $3.9 million penalty.[10] Additionally, Feinstein has been handed a corrective action plan by the OCR in the resolution agreement.[11] The ePHI of approximately 13,000 patients and research participants was exposed, including medical information of participants of research studies, lab reports, diagnoses, medications, Social Security numbers, and other IIHI such as addresses, phone numbers, and dates of birth. The OCR might not have been as strict, because no individual harm has been reported arising out of the compromised data.

Encrypt all devices containing ePHI: A major lesson from the Feinstein case is that the patients' privacy and Feinstein's money could have both been saved if the IT department had been punctilious about encrypting all electronic devices of the organization, especially the removable devices.

Insider threats: Sometimes, unauthorized access and viewing might occur due to insider error and/or malice. The annual Verizon report, Verizon 2019 Data Breach Investigations Report,[12] indicated that 27% of data breaches are caused by human error. Ironically, their study indicates that the healthcare industry is the one likeliest to be affected by insider threats and errors, with nurses, doctors, and other medical employees (e.g., receptionists, lab technicians, and pharmacists) being the most probable people to thoughtlessly click on suspicious links or view EHRs without proper authorization.

Policies and procedures: You must develop and enforce policies and procedures (P&P) to plug vulnerabilities. Give your P&P a demonstrable form by training everyone in the organization on the provisions and requirements of HIPAA and its security, privacy, and breach reporting rules. Bolster it with oversight. Evaluate any changes in the operation for their probable effect on data security and privacy. You should periodically review and, if necessary, revise your P&P, including disciplinary action to be taken against any personnel who fail to be compliant.

Prevention will be kinder to your bottom line

Those in charge of privacy and security compliance should realize the cost of prevention is less than a tenth of the cost of fines and other damages after a breach. These involve diverse kinds of safeguards that must be instituted at the policy level and enforced through appropriate procedures and regular audits. The 2018 Cost of Data Breach Study: Global Overview presented by IBM Security and Ponemon Institute[13] was the outcome of interviews conducted involving more than 2,200 IT, data protection, and compliance professionals from 477 companies that experienced a data breach in 2018 or earlier. The study indicated that in the two years following a breach, most hospitals had to increase their advertising expenditure by two-thirds to contain and counter damage to reputation.

Size doesn't protect you: Don't even imagine that only the bigger organizations are hit by cybercrimes and breaches. The Verizon report indicated that smaller institutions are likelier to be hit by a cyberattack, because they put less into resources, efforts, and time to secure their data.

Give primacy to confidentiality of all PHI and ePHI: Every healthcare institution is responsible for ensuring the confidentiality, not just the privacy, of PHI and ePHI of every patient who has visited the clinic or practice. If Atchison Hospital had been meticulous about ensuring the confidentiality of the rape victim's IIHI, then she might have been spared the horrifying consequences of the breach.

In February this year, the number of breaches may have been fewer compared to January. However, the number

of records and individuals adversely affected was humongous.[14] Three-fourths of reported February breaches resulted from IT incidents that included hacking, malware infections, and ransomware attacks. Theft of PHI and ePHI and unauthorized access resulted in only a small proportion of breaches.