Health Information Compliance Alert

Case Study: Nail Down Email Compliance Basics or Risk Exposure

Tip: Don't share your password... ever.

Much of healthcare revolves around administration, paperwork, and follow-up. And as communication in the industry has moved from a paper-based system to an electronic one, the risks for exposing both patients' protected health information (PHI) and practice secrets have increased exponentially.

Background: Last month, emails from a myriad of healthcare organizations were the cause of 13 HIPAA breaches, according to the HHS Office for Civil Rights (OCR) Breach Portal. Of the aforementioned violations, six were hijacked by hackers, and the remaining seven were due to unauthorized access or disclosure. As many as 206,994 individuals had their ePHI compromised via email-related incidents in September alone, with the majority - 155,682 of the total - attributed to hacking incidents.

It Only Takes One Email

Three violations stood out in terms of individuals impacted amongst the group of 13. All involved phishing schemes through email infiltration. They included the following large-scale HIPAA breaches:

Morehead Memorial Hospital

The Eden, North Carolina hospital reported the exposure of 66,000 individuals' ePHI on Sept. 15, 2017 due to a phishing expedition gone awry. "An unauthorized party sent fraudulent communications to Morehead, enabling them to obtain login information that allowed access to two email accounts within the hospital," noted a Morehead Memorial Hospital release on the data incident.

Unfortunately, the hacked accounts contained sensitive information from both patients and employees that ranged from "health insurance payment summaries, treatment overviews, health plan information, and in limited cases, Social Security numbers." Precautions are in place now that include a "network-wide password reset," and federal law enforcement are pursuing the cyber criminals, the news brief suggested.

Network Health

Despite "technical safeguards" in place to combat against outside invaders, two emails were the means of access for a phishing scheme that exposed 51,232 individuals. Though there was no evidence that delicate information was lost, the health insurer "took prompt action to secure the affected email accounts, to contain the impact and prevent further threats from the intruder," reported Network Health in a release.

The Menasha, Wisconsin organization added, "A forensic security expert was engaged to assess the attack and evaluate whether other areas of Network Health's network were compromised."

ABB, Inc.

The Cary, North Carolina company, ABB, Inc., updated its breach on Sept. 11, 2017. The incident impacted the ePHI of 28,012 people and was "the result of a hacker sending a phishing scheme email to ABB employees on or around August 25, 2017," noted the ABB, Inc. noticeletter, which was part of a New Hampshire Department of Justice release on the event. Of the three cases, the social engineers potentially uncovered the "name, address, Social Security number and medical record(s) used in ABB Employee Benefits [and the Family and Medical Leave Act] FMLA," mentioned thenotification.

The incident report indicated that direct deposit information for some hourly employee may have been exposed as well as the ePHI of spouses and children of employees. Due to the financial data attacked by the phishing scheme, ABB, Inc. offered those impacted "identity monitoring" as well, the notice said.

Review the statistics of these cases and the 10 others on the HHS-OCR Breach Portal at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Train Your Staff on Email

Email has been around for a long time, so it's easy to assume that your staff understands the nuances of spam, junk, or malicious threats that corrupt the practice network. But the rise in email attacks highlights that not all healthcare workers fully understand the implications.

"Although there has been a lot of recent publicity about external threats to the information systems of healthcare providers, covered entities need to also consider and proactively address threats from within their organization," such as their employees and contractors, suggests healthcare counsel **Elizabeth Hodge, Esq.** and partner attorney **Carolyn Metnick, Esq.** with Akerman LLP.

Tip: Focus on possible threats from employees and business associates (BAs) in your enterprise-wide risk assessments, and not specifically for nefarious reasons or because you think your staff might steal your patients' information. Many high-level employees including managers, clinical staff, and administrators are often the most at-risk for attack in a phishing practice known as "whaling." Social engineers oftentimes use another tactic called "spear phishing" too, which targets vulnerable or novice staff who unwittingly click and unleash chaos.

That's why you might want to "identify security threats by conducting a security risk assessment or a more thorough test of system-wide vulnerabilities," Hodge and Metnick say. If you do experience a breach, having written verification that you completed an assessment and implemented your findings with compliance protocols will go a long way in reducing the feds wrath.

"Training on data security for workforce members is not only essential for protecting an organization against cyber attacks," reminds the **HHS-OCR** in its July 2017 Cybersecurity Newsletter. "It is also required by the HIPAA Security Rule."

Follow 4 Expert Tips to Prevent This Type of Breach

This type of massive, sophisticated data breach may seem impossible to prevent - but you can actually avoid it by taking a few simple steps. In a health law blog from Ogden, Murphy, Wallace Attorneys in Seattle, attorney **Casey Moriarty, Esq.** offered the following tips:

Safeguard and Educate: This is yet another reminder to safeguard your electronic systems and educate your staff members on security policies and procedures.

Watch Staff Emails: A staff member who clicks on a link in an email or responds to an email from hackers who pose as security personnel could result in unknowingly installing the malware.

Use Encryption: Consider employing encryption technology that meets the HIPAA breach safe-harbor standards to avoid or mitigate this type of breach.

Check with IT: When staff members are in doubt about a suspicious email, phone call or other communication, instruct them to always check with your IT personnel and your HIPAA privacy officer before taking any action.

Remember Privacy Still Matters

"Also consider your workforce's privacy knowledge," Hodge and Metnick add. "Many employees do not know how to identify socially engineered emails or other security threats. Employees should be trained on identifying socially engineered emails."

And that's why technical training is essential to keeping breaches to a minimum. Most costly violations are caused by staff accidentally due to a lack of education on the HIPAA Security Rule not the HIPAA Privacy Rule. "Fix your people. They are prone to human error," recommends compliance expert **Brand Barney, CISSP, HCISPP, QSA,** a security analyst with Security Metrics in Orem, Utah.

Resource: For a look at the OCR's Cybersecurity Newsletter on phishing, visit www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf?language=es.