Part B Insider (Multispecialty) Coding Alert

Compliance: Worried About the Loss or Theft of PHI in Your Practice Due to Cyberattack?

Ensure that you and your associates understand what's at stake when PHI is compromised.

When PHI goes missing, you can't simply sweep the issue under the rug. Be sure you know exactly what to do in this situation before it happens□or you could be in a world of trouble.

Promoting safety and securing patients' welfare are the hallmarks of concerned providers, but sometimes accidents happen and occasionally criminals are involved. When protected health information (PHI) is lost, whether by accidental oversight or by thieves intent on disrupting the system, it is a serious matter and should be dealt with immediately.

Background. This past June, it was discovered that a criminal by the name "darkoverlord" hacked into a myriad of health care partner systems, wreaking havoc and threatening to expose the PHI of over 650,000 patients, a HotHardware.com article states. Spanning the nation from the Midwest region to areas in the south, the breach is huge in scope, and the perpetrator is trying to sell the compromised data online for upwards of $400,000.

Due to the significance of the attack, CMS issued a Special Edition MLN Matters release reminding providers to engage with business partners who understand and utilize the best HIPAA-compliant practices.

Why this matters. "Lost or stolen PHI should be taken seriously because, among other reasons, HHS takes it very seriously. HIPAA's Breach Notification Rule requires reporting of a breach of unsecured PHI to the individuals and the secretary of HHS and, if a breach affects more than 500 individuals, to the media," **Michael D. Bossenbroek, Esq** of Wachler & Associates, PC in Royal Oak, Mich., explains. "This rule also requires business associates to notify the covered entity as well if they are responsible for a breach. Breaches can lead to HHS investigations and compliance reviews."

Cyberattacks Are Happening More Often

As the realm of health care and the businesses that service the industry widen, the opportunity for lost PHI rises. Due to the expansion of digital resources for health care providers to assist their patients, cyberattacks have become more prevalent and are a dangerous threat to patients' and providers' safety and security.

Increased settlements. "With increasing frequency, HHS is announcing significant six- and seven-figure settlements with covered entities and business associates," Bossenbroek says. "These settlements, although they uncovered other problems, often originated with stolen or lost PHI."

ONC data revealed. Recently, the ONC reported that criminal cyberattacks are on the upswing with an increase of 125 percent over the past five years, "replacing employee negligence and lost or stolen laptops as the top cause of health care data breaches. The average consolidated total cost of a data breach was $3.8 million, a 23 percent increase from 2013 to 2015," **Karen B. DeSalvo, MD, MPH, MSc**, national coordinator for health IT and HHS assistant secretary for Health and **Nicole Lurie, MD, MSPH**, assistant secretary for preparedness and response, said in a joint ONC press release on July 25, 2016.

What's ahead. Unfortunately, the frequency and magnitude of this high-tech mayhem cannot be ignored. With the onset of MACRA and quality-centered care that utilizes more-sophisticated CEHRT through ACI, the possibility of more profound breaches is likely.

It will be crucial to know your business associates, "particularly those providing or maintaining the software and hardware handling your PHI," Bossenbroek says. "It will not be enough to simply check the box that a BAA is in place.

The covered entity should know their business associates and understand what issues, if any, they are having with handling PHI."

"If integrated models are the future and will reshape how providers interact and communicate with each other, the transmission and storage of ePHI among covered entities will be a vulnerability that may stretch the Security Rule as well," he explains.

Here's What You Can Do to Protect Yourself

There are things that you and your staff can do to protect yourself against health care cyberattacks, ransomware, and other digital warfare. Here are some tips to help you protect PHI and what to do should you discover a HIPAA breach:

- Educate yourself and your staff on the HIPAA Privacy Rule and Breach Notification Rule. A clear understanding of what PHI is and how to protect it as well as how to report the loss of it through the various avenues and tools the HHS offers.
- Keep abreast of cyberattack news through the ONC, OIG, and HHS updates.
- Familiarize yourself with the modus operandi of hackers to ensure you can recognize if your patients' PHI has been compromised.
- Report immediately any HIPAA violation of lost or stolen PHI to the authorities. This early outreach may reduce any civil or criminal liability on your behalf.
- Research thoroughly the background of any and all business partners you associate with and insist upon arranging a HIPAA-compliant business associate agreement (BAA).

Final note. As more settlements arise from this type of PHI loss, more penalties will ensue, both monetary and criminal. The other outcomes can be just as staggering.

"This [monetary and criminal penalties] does not even take into consideration the reputational harm to the institution, the loss of public trust, and the potential embarrassment, inconvenience, and harm to patients and their families," Bossenbroek points out. "All of this occurs in the very hostile environment of cyberattacks, ransomware, and even the threat of insiders, which HHS has been warning the industry about."

Resources: For a link to the Special Edition of MLN Matters on PHI and HIPAA, visit https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/SE1616.pdf.

For a closer look at the ONC's press release on addressing cyberattacks, visit https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/opportunity-sharing-information-cyber-attacks/.