Codify
BY AAPC

Health Information Compliance Alert

Data Security: Lack of Cybersecurity Skills Often Leads to Digital Mayhem

When your EHR system is under siege, the losses are more than just financial.

Hackers are the pests of the healthcare industry. And, when you least expect it, they sneak right in through the back door like a fly on a hot, summer day. With the click of a mouse and without invitation, they create cyber chaos.

Looks Like 2017 is Off to a Rough Start

The healthcare industry's digital welfare has already suffered some blows for CY 2017. According to the OCR and HHS breach portal, seven large-scale hacking or IT incidents have been reported. The breaches affected unsecured PHI and ranged from 600 individuals to 24,809. Here is the link to the OCR breach portal: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Even though the OCR has not gone into detail about the incidents, the largest one affecting 24,809 individuals at WellCare Health Plans and disclosed on Jan. 27, 2017, was related to an earlier ransomware attack on Summit Reinsurance Services from August 2016 that exposed sensitive information.

Source material. The ONC reported last July that criminal cyberattacks were 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 healthcare data breaches. The average consolidated total cost of a data breach was $3.8 million, a 23 percent increase from 2013 to 2015," a 2016 ONC press release suggested.

"Cybercriminals will always be drawn to where the money is, so healthcare organizations will continue to be a target due to the highly sensitive, and highly profitable, electronic protected health information (ePHI)," warns **Ken Adamson**, vice president of product management for Proficio. "In 2015 alone, one in three Americans had their health records breached."

"As more stolen patient records saturate the black market, however, hackers are turning to other methods of attack, such as ransomware," Adamson adds. "Healthcare organizations are more likely to pay the ransom than other industries, given the potential life-or-death implications of having critical systems down."

Reminder: In one of the most talked about cases over the past year, Hollywood Presbyterian Medical Center in Southern California was hijacked by cyber criminals for ten days. The computer systems were held for ransom and were not released until the hospital paid 40 bitcoins, about $17,000.

Here's the recompense. In this case, the sum paid out was nothing compared to the inconvenience of patients and staff in addition to the financial loss of being out of business for ten days. >

"The Hollywood Presbyterian incident has been a huge wake-up call for healthcare and has finally allowed information security to have the respect it deserves in the boardroom," notes HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, VT. "Healthcare has traditionally been less sophisticated when it comes to information security ... [but] now is the time to get serious about protecting systems, because lives and institutions are at stake."

Don't Get Overwhelmed

The list of things to avoid, the constant IT alerts, the HIPAA rules that must be followed, the protective software all of these things can bring on compliance overload. Oftentimes, trying to cover all your bases at once makes you more vulnerable and open for a cyber attack.

"The sheer volume of security alerts generated each day, many of which are false positives, increases this risk as valid security alerts can easily slip through the tracks," Adamson says. "IT teams simply don't have thebandwidth to supply around-the-clock protection andinvestigate each threat properly. In an industry where it takes over 200 days to identify a breach, every second matters."

Outline a Plan and Stick to It

Once you've discussed and assessed the threats to your office system, design an action plan that your staff can understand and work with. Take into account these pointers as you strategize ways to combat a ransomware attack:

- Train your staff on the importance of cybersecurity.
- Keep all systems secure.
- Back-up your practice data often.
- Track network traffic and look for inconsistencies.
- Limit access to ePHI.
- Adopt alternative measures and protections to keep ransomware at bay.

Note: Promoting safety and securing patients' welfare are the hallmarks of concerned providers, but sometimes accidents happen and occasionally criminals are involved. When PHI is lost, whether by accidental oversight or by online attack, it is a serious matter and should be dealt with immediately.

Resources: For more information about the OCR's guidance on ransomware, visit https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.