Codify by AAPC

MDS Alert

Cybersecurity: Don't Fall Prey To These Device Mistakes

Innocent mistakes are just as problematic as nefarious action.

With everything increasingly device-centric, cybercriminals are on the lookout for ways in which they can attack. Save yourself and your organization time, money, and stress by going on the offensive with education and security.

Try these five questions to figure out where any cyber-weakness might be.

Question 1: Everyone who works on the MDS in your facility is crazy about this new resident-driven payment system (PDPM) blog that offers tips and advice. The nurse assessment coordinator and therapy staff frequent the site throughout the workday from their various devices around the facility. But, after months of utilizing the online resource, staff computers start to lag and employees have problems downloading information. One Monday morning, the entire group is locked out of the system. What might have happened?

Answer: What may have transpired involves two different, but similar, forms of phishing techniques aimed at preying on providers' habits. Nurse assessment coordinators, who spend increasing time looking up ICD-10 codes repeatedly on the same site, may end up being targeted by "pharmers," while a group of MDS contributors researching a particular topic are usurped by the "watering hole" tactic.

Both harness common interests and log how often a site is visited. Hackers use the information to either direct you to an identical but false page, stealing your passwords and controls, or install malware to the popular link and infiltrate your office system with it. Once inside your network, cyber criminals can wreak all sorts of havoc, including hijacking of residents' electronic protected health information (ePHI).

Question 2: Every day when you log into your laptop, a little reminder pops up asking you to install the latest Microsoft patch for the software your facility utilizes. Your IT manager says just click "remind me tomorrow," but tomorrow turns into weeks. Before you know it, the entire facility network is down. What could have stopped the outage?

Answer: Software patch management and stricter security protocols could have closed up the loophole that let hackers in. Technology coordination between vendors and health IT staff ensures compliance. And more importantly, healthcare continues to be ravaged by the lack of patch maintenance, which then breeds chaos throughout the industry.

"Cyber criminals prey upon lax security practices; most breaches and attacks are preventable through a higher prioritization of operational security, including patch management and aggressive training programs," observes **Kurt J. Long**, founder and CEO of **FairWarning** in Clearwater, Florida. "Apply vendor recommendation patches aggressively, and watch for vendor updates vigilantly."

Tip: "Not only should your IT team remain on top of such updates, but also, they should be driving a security-centric culture through your organization," Long advises.

Question 3: You just moved from a rural, independent facility to an urban facility that is part of a larger corporation. Your IT person approved the use of your personal devices under the organization's Bring Your Own Device (BYOD) policies, but he insisted that software to monitor practice data be installed for security reasons. Why?

Answer: Smartphones, laptops, and tablets allow staff to access work anywhere and at any time. However, despite this convenience, lost and stolen devices accounted for a significant number of breach cases over the last few years across the healthcare industry, exposing millions of people's ePHI.

Large-scale medical systems now utilize mobile device management (MDM) software and governance to protect assets and residents. Certified EHR Technology (CEHRT) vendors offer additional coverage of mobile devices with applications to help providers combat this common issue, too. The **HHs office for Civil Rights** (OCR) and the **HHs office of the national Coordinator for Health information technology** (ONC) also provide advice and insight on how to implement compliant MDM programs.

Question 4: The facility where you cut your teeth on MDS is closing, and you move to a new facility in a different state with new administrators and staff. When your old boss closes the facility, an administrator throws the old software, hardware, and paper files into the dumpster since you won't need the materials or the data anymore. What's wrong with this scenario?

Answer: Everything! The feds have specific instructions for how PHI and ePHI should be disposed of, whether a healthcare facility is open or closed. In fact, OCR advises covered entities (CEs) strictly follow risk management protocols when dealing with information after a business goes under.

Some of its suggestions include:

- Shred, burn, pulp, or pulverize records that contain PHI, ensuring that the information is thoroughly indecipherable and destroyed.
- Clear, destroy, wipe, overwrite, purge, and destroy any electronic media that contains ePHI.

See the OCR's PHI and ePHI disposal advice at www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html?language=en.

Warning: "Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI," reminds OCR guidance. "Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member."

Question 5: Mr. Duncan abruptly departs your practice after 20 years on staff working on the MDS. During a routine systems check, your IT manager notices remote log-in access and irregularities. What may have occurred?

Answer: In this example, there's a possibility that Mr. Duncan illegally accessed the network for nefarious reasons for things as varied as stealing facility secrets to the theft of residents' ePHI. Small organizations are often too trusting while big healthcare groups may be too busy to notice the comings and goings of employees. And because so much of an organization's information is stored on its network servers, they are a liability and ripe for cyberattacks.

"Network servers are great targets for hackers because they can count on stealing a lot of information at one time from a server, while there might only be a subset of that information on a laptop, and only be a few records in an email," explains **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah.

This kind of entry into a facility's records allows cyber thugs to wreak all kinds of havoc. "If a hacker can gain access to an organization's network, they can make their way to a network server and export the data stored there - or a copy of the data - to a server outside the organization's network, and under the hacker's control," Stone warns.

Tip: Though healthcare remains a focus point for hackers, practices can use their risk assessments to look at network server issues. There are perennial problems to look for, Stone suggests. "Network vulnerabilities I see regularly include unpatched systems, shared account credentials, remote access to ePHI that only requires a username and password (no multifactor authentication), and insufficient malware protection."