Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

HIPAA Security: Set Up Stellar Remote Work Policies to Avoid HIPAA Fallout

Caution: Remote workers are hackers' dream targets, feds say.

Despite the ramped-up COVID-19 vaccination rollout, the pandemic is expected to stretch into 2022. That means that many in the healthcare industry will continue to assist patients virtually from their homes. But, just because you and your staff are working remotely doesn't mean that you can let HIPAA fall to the wayside.

Why? Despite a pandemic, cyberattacks have remained prevalent in healthcare. One of the main drivers is the increase in remote work.

"Most healthcare organizations were completely unprepared to work from home securely when the pandemic hit," says **Jen Stone, MCIS, CISSP, CISA, QSA,** principal security analyst with Security Metrics in Orem, Utah. "Most made valiant attempts to make do with what they had, engaging in an emergency mode that probably wasn't prepared for extensive remote work," she adds.

"However, with lockdowns dragging on and working from home continuing for the foreseeable future, we can't continue to cross our fingers and hope that a breach won't happen," Stone acknowledges.

In fact, a recent bulletin from the Cybersecurity and Infrastructure Security Agency (CISA) titled "Cybersecurity Challenges to the Healthcare Sector, Independent of and Due to COVID-19" suggests several factors make remote workers more vulnerable to data security incidents.

Reminder: CISA works with other federal departments to protect the country's infrastructures and encourage cybersecurity. Additionally, the National Risk Management Center (NRMC), which is a part of CISA, works in tandem with partners and stakeholders to "analyze, prioritize, and manage the most strategic risks" in the nation, CISA online guidance suggests.

In its bulletin, CISA points out a variety of issues that are worrisome for remote workers in the healthcare industry:

- **Staff training:** Remote workers lack the necessary skill set to identify IT issues.
- **Updates:** Staff likely don't know how to manage software updates, cloud technologies, or other programs necessary to work at home.
- **Incident response:** If employees weren't properly trained to recognize a malware, phishing, or vishing attack before they started working from home, it's likely that they don't know how to respond to or address a remote hack.
- **Endpoint security:** In an office, staff rely on IT management to secure and protect computer networks. At home, the compliance is up to the remote worker - and this heightens the chance of a breach.

These remote work challenges have made securing protected health information (PHI) during the time of COVID-19 even more difficult. In addition, "PHI is estimated to be worth 10-20 times the value of credit card data on the Dark Web, and is sought after by criminals and nation-states alike," CISA warns in the release.

"It's critical for healthcare organizations to protect their remote staff with the same rigor as in the office," says Stone.

"This means using company-issued laptops for work only, extending the existing protected network (e.g., through use of a VPN), and ensuring that endpoint security controls such as antivirus, patching, logging, etc., are centrally managed so that IT personnel can ensure updates are happening," she reminds.

And if any of the HIPAA breach settlements have taught covered entities (CEs) anything over the past year, it's the importance of assessing, analyzing, and managing risks as outlined in the HIPAA Security Rule.

"Every year, healthcare organizations should be conducting a meaningful risk assessment and re-evaluating contingency planning," Stone advises. "This year offers a unique opportunity to leverage these activities in a way that ensures the confidentiality, integrity, and availability of protected health information in any situation."

Resource: See the CISA bulletin at www.cisa.gov/sites/default/files/publications/202012220800_Graphic_Challenges_to_Healthcare.pdf.