Health Information Compliance Alert

Cybersecurity Toolkit: Hammer Out Comprehensive Texting Rules for 2021

Tip: Teach staff to pause and think before they click.

With COVID-19 forecasts predicting a long, difficult winter, you may be considering going back to offering predominantly digital care via telehealth for your patients. Before you send your staff home to work remotely, you may want to address mobile device rules and secure texting protocols.

Here's why: COVID-19 scams are on the rise. Scammers are using text messaging that looks official, pretending to be government agencies, vendors, or financial institutions to lure recipients to click on the link, according to a **Federal Communications Commission** (FCC) alert on Nov. 19. "As the COVID-19 pandemic continues to impact the United States, the FCC has learned of scam text-message campaigns and robocalls that prey on virus-related fears," notes the FCC alert.

Along a similar vein, the **HHS Office of Inspector General** (OIG) also updated its COVID-19 scam site on Dec. 3. Additionally, OIG points out that "fraudsters are offering COVID-19 tests, HHS grants, and Medicare prescription cards in exchange for personal details, including Medicare information. However, these services are unapproved and illegitimate," the watchdog agency warns.

Add These Tips to Your Texting To-Do List

Healthcare workers aren't exempt from falling into the clutches of cyber criminals. In fact, both the **Cybersecurity and Infrastructure Security Agency** (CISA) and the **Federal Bureau of Investigation** (FBI) have warned repeatedly about ransomware, phishing, and other cyber attacks targeting the healthcare industry specifically (see Health Information Compliance Alert, Vol. 20, Nos. 9 & 11).

And with more and more work being done outside the confines of an office and on mobile devices, it's fairly easy to become the victim of a texting hack - and expose not only practice data but patients' electronic protected health information (ePHI).

"Healthcare was already turning to texting, but COVID-19 dramatically increased that form of communication, probably before most organizations were ready for it," says **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with **Security Metrics** in Orem, Utah.

Caveat: Because the world relies so heavily on mobile devices to transfer data and relay messages quickly, many may not even consider a stray text here and there a worry - but they'd be wrong, Stone warns. "On top of other security issues with SMS, we have to be ready for phishing over text (also called smishing). Smishing is sneaky because we aren't trained to look for malicious activity on our phones, which means we're more likely to click on links that come to us through texts," she cautions.

There are some things you can do to prepare your staff. First, you need to educate your employees on both the tactics and the risks to ePHI. "Organizations need to train users not to click, even if they think they know who is sending the

link," Stone advises.

Nowadays it's hard to avoid using mobile devices to send and receive ePHI - especially during the pandemic and with healthcare workers siloed at home. If you can help it, "it's best not to use mobile devices for sending or receiving ePHI," Stone maintains. "But, communication can be done in a HIPAA-compliant manner if mobile devices are properly secured, and if the information shared is limited," she says.

Stone also recommends checking out federal guidance. "The **Office of the National Coordinator for Health Information Technology** [ONC] offers excellent advice for securing mobile devices on the HealthIT.gov site," she says. Some of the ONC's mobile device management tips include advice on password controls, remote wiping protocols, encryption, security updates, and deleting stored health information from devices daily.

Resource: Check out the ONC guidance at www.healthit.gov/ topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device.