Codify
BY AAPC

MDS Alert

Cybersecurity: Don't Let Mobile Device Vulnerability Cause Security Breaches

Though management may want key employees to be able to access information outside the office, mobile devices are risky without proper precautions.

Smartphones, tablets, and laptops are essential to any successful business in today's market. But, if you don't take precautions to keep data safe, you could end up in hot water, endangering your patients and impacting your bottom line.

Expert insight: "Using a smartphone with PHI [protected health information] requires that the devices be set certain ways to secure information and allow remote control of the device should it become lost or stolen," stresses HIPAA expert **Jim sheldon-Dean**, founder and director of compliance services at **Lewis Creek systems LLC** in Charlotte, Vermont. "While a small office can get by with just a policy that says what a user should do; a larger organization will need to establish a mobile device management [MDM] solution that allows the devices to be managed by IT, not the user."

Fortunately, there are strategies that you can employ to help protect your mobile devices and your patients' protected health information (PHI).

Rely on these strategies provided by the Department of Health and Human Services **Office of the National Coordinator for Health information technology** (ONC) to ensure your facility's mobile devices stay safe and secure.

Determine device usage

First, decide whether you'll use mobile devices to access, receive, transmit, or store patients' PHI - and outline who will be in charge of the management and maintenance of the devices. Also, resolve whether you'll integrate smartphone and tablet utilization as part of your facility's internal network or systems.

Also evaluate who will be using the facility's network or systems, generally. Do residents' family have access to Wi-Fi when visiting? Do visiting physicians respond to emails from their personal devices when they're not physically at the facility?

Calculate the risks

Consider the risks of using mobile devices to transmit PHI. Conduct a risk analysis to identify threats and vulnerabilities.

Outline a risk management plan

Using the information garnered from your risk assessment, establish a compliance strategy pertaining to your mobile devices, taking into account the HIPAA Privacy and Security Rules. This MDM game plan willhelp your office develop and implement safeguards, reducing problems previously identified in your risk analysis.

Tip: Remember, your compliance planning should include frequent evaluations and regular maintenance of the mobile device safeguards you put in place.

Implement HIPAA-compliant policies and procedures

Design and develop mobile device policies and procedures with clear-cut documentation, keeping HIPAA in mind. Ensure that your protocols address MDM, bring your own device (BYOD) issues, and restrictions on personal use. Management of applications, security, and configuration settings for mobile devices must be maintained, too.

Educate employees

Provide mobile device privacy and security training for all staff members on an ongoing basis. Educate employees from the bottom to the top on what your facility rules entail, on HIPAA compliance and MDM, and what a violation means for the facility at large, as well as team members.

Resource: For more ONC advice on managing your practice's mobile devices, visit www.healthit.gov/sites/default/files/mobile_devices_and_health_information_privacy_and_security.pdf.