Health Information Compliance Alert

Toolkit: Implement Strong MDM Protocols to Ensure HIPAA Compliance

Hint: Make encryption a priority.

Smartphones, tablets, and laptops are essential to running a successful medical practice 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' PHI. Follow these five steps to keep your practice compliant.

Utilize MDM Advice from the ONC

The HHS Office of the National Coordinator for Health Information Technology (ONC) offers the following steps to ensure your practice mobile devices stay safe and secure:

1. Determine device usage: First, decide whether you'lluse mobile devices to access, receive, transmit, or store patients' PHI - and outline who'll be in charge ofthe management and maintenance of the devices. Also, resolve whether you'll integrate smartphone and tablet utilization as part of your practice's internal network or systems.

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

3. 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 will help 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.

4. 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.

5. 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 office rules entail, on HIPAA compliance and MDM, and what a violation means for your practice.

Tighten Mobile Device Security

Here are some tips to secure PHI on mobile devices, also courtesy of the ONC:

- **Set strong passwords:** Always use a password or other user authentication on mobile devices. Multi-factor authentication passwords are recommended.
- **Encrypt:** Install and enable encryption to protect health information stored, utilized, or sent by mobile devices.
- **Use automatic log off:** Also, make sure your mobile device requires a unique user ID for access.
- **Enable remote wipe:** Install and activate wiping and/or remote disabling to erase the data on your mobile device if it is lost or stolen
- **Keep the device with you:** Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use.
- **Use a screen shield:** Don't share your mobile device with anyone, lock the device when not in use, and implement at-rest protocols.
- **Install a firewall:** Install and enable a firewall to block unauthorized access.
- **Use a secure Wi-Fi connection:** Use adequate security to send or receive health information over public Wi-Fi networks.
- **Research mobile applications before downloading:** Disable and do not install or use file-sharing applications.
- **Employ security software:** Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks. Keep your security software up to date.
- **Use proper disposal methods:** Delete all stored health information on your mobile device before discarding it.

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.