Codify
BY AAPC

Health Information Compliance Alert

Don't Forget to Make Accommodations for HIPAA When You Text Patients

Tip: Encrypt your mobile devices to lessen the chance of a breach.

Mobility is a clear focus in healthcare today, and it goes hand-in-hand with patient engagement because of its ease of use and widespread adoption. However, there are shortcomings with the rise of mobile healthcare, and those problems fall heavily under HIPAA.

Convenience vs. liability: There are drawbacks to the texting renaissance. Oftentimes, the convenience of mobile implementations begets staff complacency where the line between what is acceptable and what is a violation gets blurred. And when this happens, HIPAA violations occur. Incidents in the past have been as innocent as a text or social media post that's become fodder for a breach to the loss of an unencrypted smartphone that leads to the takedown of an entire hospital system.

Caveat: There's a shift in healthcare that suggests providers up their availability as a resource and caregiver to their patients or risk financial losses. MACRA's Quality Payment Program requires clinicians and their staff to put the patient first. Though it is the first year of the federal reimbursement plan, private payers are sure to follow.

What That Means to You

These new initiatives promote the ideas behind patient engagement open lines of communication between provider and patient, access to health records and care information, and policies, procedures, and services that enhance the overall healthcare experience. All that suggests mobility will continue to be at the forefront of patient access.

Bottom line: SMS texting is not encrypted or secure, yet clinicians and their staff text each other and their patients ePHI, putting everyone at risk. These practices are vulnerable to cyberattacks and the loss of data.

So, if your office engagement includes text blasts and mobile-friendly apps, ensure that you protect yourself and your patients with HIPAA-friendly protocols. Look for "apps for HIPAA-compliant texting that meet healthcare industry standards for security and privacy during the communication of ePHI," says **Michael DeFranco**, founder and CEO of Lua. "Additionally, with text messaging, and due to the features included in secure messaging solutions, it ensures that system administrators can audit access to encrypted ePHI and any transmission of confidential data in compliance with HIPAA regulations."

Reach out to your patients, but consider ideas to assist in your office HIPAA-compliant texting plan:

- Train your staff to combat the accidental loss of ePHI and to look for cases where the exposure is intentional.
- Implement mobile tools that are easy-to-use, linked to your CEHRT, and are HIPAA compliant.
- Separate personal texting from practice texting to avoid issues and enforce the policy.
- "Eliminate the threat of sensitive data being compromised if a mobile device is stolen or lost with message recall, message lifespan, and remote wipe," says DeFranco.
- Utilize multi-factor authentication and encryption techniques.
- Ensure that all your mobile devices have at-rest security options.

Resource: For more information about HIPAA-secure texting, visit https://getlua.com.