Part B Insider (Multispecialty) Coding Alert

Compliance: Is Your Practice Texting in Line with HIPAA Standards?

Ensure that you're protecting yourself and your patients when you text.

Mobility—it is both the boon and bane of the health care industry and the greater society. On one hand, smartphones and tablets have allowed providers to assess patients with the mighty power of the net and all of its knowledge at their fingertips. These products have also helped doctors coordinate care between venues and specialties as well as transfer their notes quickly to staff, making the coding and billing process quicker and more efficient.

But, this communication revolution has its drawbacks, too. The handy nature of these implementations makes people complacent, and the line between what is acceptable and what is illegal is often blurred. The ease of use allows both clinicians and administrative staff to transfer data, voice opinions, and send private patient and practice information any which way they choose. When this happens, an innocent text could become fodder for a Health Insurance Portability and Accountability Act (HIPAA) breach.

Background. The U.S. Department of Health and Human Services (HHS) requires that all covered entities—health care providers, health plans, and health care clearinghouses—follow strict mobile-use guidelines under the HIPAA security rule. The rule lists a detailed inventory of governmentally-mandated requirements that are meant to help preserve electronic protected health information (e-PHI). Some of the highlights focus on setting up administrative, technical, personal, and physical safeguards to protect all involved parties. (http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html).

Since Medicare payment has been tied to adopting certified electronic health record technology (CEHRT) for a while now due to its necessity in the delivery of quality care, most providers and their partners have jumped on board the cyber train lest their incomes be inhibited.

"Since the implementation of the Affordable Care Act (ACA) and Meaningful Use (MU), medical providers are relying on cost effective services that take pay-for-performance into consideration. These services include texting, telemedicine, and outsourcing," explains **Michael DeFranco**, founder and CEO of Lua, a leader in health care mobility. "The growth of innovative technologies can lower the cost of delivering healthcare, and provide for better patient outcomes and patient satisfaction."

The upside. Texting in particular speeds the daily work flow, connecting physicians, staff, and business partners with the easy distribution of information. Its efficiency and cost effectiveness can successfully reduce readmissions, coordinate the management of chronic care, help with e-Prescriptions, and increase and improve patient engagement, suggests DeFranco.

Here's the Problem

Unfortunately, messaging abuses have become a serious problem for the health care industry, and the OIG is on the watch for violators of these HIPAA security rules. Lax office procedures, the enticement of a financial windfall from information theft, and workers with a lack of compliance education have increased the likelihood of cyber villainy and the loss of ePHI.

It's more than a quick fix. "Since providers text their patients and other providers ePHI, which should never be

transmitted in an unsecured manner, they need a solution," says DeFranco.

Training matters. The first step your practice should take involves devising a comprehensive plan that includes realistic procedures to combat the accidental and intentional loss of ePHI. Educating administrative and clinical staff on the rules related to HIPAA-compliant communication via text, interoffice messaging, and email is essential to keep your practice safe and secure. Integrating HIPAA-compliant, user-friendly software and applications across the different mobile products your group utilizes is crucial to the success of your overall plan.

"Apps for HIPAA-compliant texting meet health care industry standards for security and privacy during the communication of ePHI," says DeFranco. "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."

Look For HIPAA-Compliant Apps with These Important Features

Here are seven things DeFranco suggests practices have set up before they add texting to their office dynamic:

- Eliminate the threat of sensitive data being compromised if a mobile device is stolen or lost with message recall, message lifespan, and remote wipe.
- Segregate healthcare texting from personal texting through a HIPAA-compliant, secure application.
- Encrypt message data in-network and in-transit on the device and the server.
- Look for a lockout feature that erases data remotely if devices are stolen.
- Require PIN authentication for all application users.
- Include configurable time-out periods.
- Block users after a number of unsuccessful authentication attempts.

Bottom line. SMS texting is not encrypted or secure, yet providers unwittingly engage in the practice of texting often, leaving their patients and themselves vulnerable to cyberattacks and the loss of ePHI. Due to the confusing nature of the policies, it is wise to seek the advice and assistance of health care IT experts schooled in the complexities of the HIPAA security rules and regulations.

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