Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: Weigh The Pros & Cons Of Communicating With Patients Via Texting

Check out these 'HIPAA compatible' text messaging Apps.

Text messaging is a common communication method for most Americans these days, but text communications that include protected health information (PHI) can pose a whole host of risks to privacy. Don't risk a HIPAA breach with your text messages here are the decision points you need to consider before using texts to communicate with patients and what you can do to mitigate the risks.

Is Texting Right for Your Patients?

"With the proliferation of mobile technologies and a steady shift toward smartphone interactions as a predominant mode of communications for many consumers, you may be considering texting as a more effective and efficient way to communicate among providers and/or with patients," attorney **Michelle Caswell**, JD said in a recent blog posting for **Clearwater Compliance LLC.**

Texting is a fast way to communicate short messages to patients, such as updates and schedule changes, according to **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT.

And in some cases, texting may be more appropriate than sending an email or making a phone call, Sheldon-Dean points out. For example, texting can be more discreet and private than a phone conversation that someone could overhear. Texting is sometimes quicker than a phone call for short messages and can provide accurate information not dependent on voice.

In the past, many healthcare professionals would use pagers, but now texting has become a better option, Sheldon-Dean says. Many paging operations are moving to texting now, and texting is more interactive than paging.

2 Big Issues with Texting

The biggest, overall HIPAA-related issues with text messaging are privacy and documentation. Consider these issues carefully before deciding to use texting in your patient communications.

1. Privacy: Patients may not appreciate the risk of privacy loss through texting, Sheldon-Dean warns. Also, texting is a new technology and people will not understand it fully for quite some time.

"HIPAA does require you to do your best to meet patient preferences for communication methods," Sheldon-Dean reminds. You must use a Risk Analysis to evaluate and explain the risks to patients, Sheldon-Dean advises.

2. Documentation:"Regular texting doesn't provide a paper trail of conversations and contacts," Sheldon-Dean says. If a communication is part of patient care, you must document it properly, and that requires more than regular texting. A secure, traceable texting technology is important when you're texting medical record information.

If PHI is included in texts between you and your patient, "the messages may be subject to HIPAA in more ways than just security," Caswell agreed. You may need to save texts for a legally required time period, allowing the patient to access and amend the text messages. And if you choose to delete the texts for security purposes, you may be violating HIPAA's retention requirements.

Weigh the Risks of Texting Carefully

Many things can go wrong when it comes to text messaging with patients or other providers. For example, you might end up providing information to the wrong person due to poor authentication and access controls, Sheldon-Dean warns. This situation would lead to a "small" breach and a healthcare threat.

Or you could accidentally provide incorrect information about a patient, "perhaps by faulty authentication or a poorly performing App, causing a healthcare threat," Sheldon-Dean cautions. And if you use an unsecured text messaging App, data may remain and be accessible on systems.

Another problem: What if the patient loses his device, exposing his data? This is the patient's problem, but what if the device loss potentially exposes additional data or provides faulty data? What if you or one of your employees loses control of a device, potentially exposing extensive data? This is a big problem. And an even bigger problem is if the device loss potentially provides access to your systems.

Follow 5 Tips to Create Effective Texting Policies & Procedures

If after weighing the pros and cons your practice decides to communicate with patients via text, you should implement policies and procedures that establish safeguards and reduce liability exposure, Caswell said. Caswell offers the following tips for creating solid policies and procedures:

1. Include only non-urgent information. If you're texting with a patient, include only non-urgent information like appointment reminders or prescription refills. If you have a secure patient portal, you could use text messaging simply to alert the patient to a message in the portal.

2. Don't communicate identifiable information. Avoid texting any information that is specific and identifiable to the patient, such as patient ID numbers, treatment details or names of conditions.

3. Double-check the number. Always ensure that the number you're using to contact the patient is the appropriate number to send texts.

4. Include treatment texts in the medical record. If texts are related to patient treatment, you must include the contents of the texts in the patient's medical record.

5. Put a mobile device management plan in place. Your mobile device management plan should include:

- Encryption of mobile devices;
- Password protection;
- Guidelines on whether employees can use their own devices or if they must use only company-owned devices;
- Monitoring/audit of all text messages; and
- Use of applications that will allow the phone to verify a device prior to sending (similar to credit card companies that allow you to verify your phone prior to sending data).