HIPAA Compliance for Clinician Texting

Save to myBoK

By Adam H. Greene

The HIPAA privacy and security rules need not act as an obstacle to efficient communications, but keeping texting compliant requires planning and diligence.

Text (or SMS) messaging has become nearly ubiquitous on mobile devices. According to one survey, approximately 72 percent of mobile phone users send text messages.[1] Clinical care is not immune from the trend, and in fact physicians appear to be embracing texting on par with the general population. Another survey found that 73 percent of physicians text other physicians about work.[2]

Texting can offer providers numerous advantages for clinical care. It may be the fastest and most efficient means of sending information in a given situation, especially with factors such as background noise, spotty wireless network coverage, lack of access to a desktop or laptop, and a flood of e-mails clogging inboxes.

Further, texting is device neutral-it will work on personal or provider-supplied devices of all shapes and sizes. Because of these advantages, physicians may utilize texting to communicate clinical information, whether authorized to do so or not.

It is essential for healthcare providers to understand the communication needs of their workforce in order to appropriately address any privacy and security risks they may pose. As many providers have discovered, trying to control how your workforce communicates is easier said than done, and policies that fail to account for clinicians' communication preferences often go unheeded.

This article addresses texting between clinician members of the workforce and discusses how to ensure safer texting practices as part of your organization's privacy and security compliance program.

The Risks of Text Messaging

All forms of communication involve some level of risk. Text messaging merely represents a different set of risks that, like other communication technologies, needs to be managed appropriately to ensure both privacy and security of the information exchanged.

Text messages may reside on a mobile device indefinitely, where the information can be exposed to unauthorized third parties due to theft, loss, or recycling of the device. Text messages often can be accessed without any level of authentication, meaning that anyone who has access to the mobile phone may have access to all text messages on the device without the need to enter a password.

Texts also are generally not subject to central monitoring by the IT department. Although text messages communicated wirelessly are usually encrypted by the carrier, interception and decryption of such messages can be done with inexpensive equipment and freely available software (although a substantial level of sophistication is needed).[3]

The HIPAA privacy rule provides an individual with the right to access and amend protected health information (PHI) about the individual that is maintained in a designated record set.[4] The designated record set includes PHI "used, in whole or in part, by or for the covered entity to make decisions about individuals."[5]

Accordingly, if text messages are used to make decisions about patient care, then they may be subject to the rights of access and amendment. There is a risk of noncompliance with the privacy rule if the covered entity cannot provide patients with access to or amend such text messages.

Include Texting in Compliance Programs

Under the HIPAA security rule text messaging may be addressed as part of an organization's comprehensive risk analysis and management strategy.

As part of its risk analysis, a healthcare provider may identify where electronic PHI, or ePHI, is created, received, maintained, and transmitted.[6] For texts, ePHI will primarily be created, received, and maintained on mobile phones (although text messages may also reside on workstations or cloud-computing servers).

Texts also may be temporarily maintained on a telecommunications provider's servers while the message awaits delivery to the recipient's device (e.g., if the recipient's device is powered off or out of range). Texts primarily will be transmitted through the wireless cellular networks of telecommunications providers, although they also may get routed through the Internet in certain situations.[7]

The next step is to identify and document any reasonably anticipated threats to ePHI, the security measures already in place (e.g., an existing policy on texting), the likelihood of each threat, and its potential impact.[8] Examples of threats include:

- Theft or loss of the mobile device
- Improper disposal of the device
- Interception of transmission of ePHI by an unauthorized person
- Lack of availability of ePHI to persons other than the mobile device user

It is worth keeping in mind that the threat of external interception is likely far smaller than the threat of theft or loss of the device.

Based on the above risk analysis, a provider can determine the appropriate administrative, physical, and technical controls for the organization. Examples of security controls include:

- An administrative policy prohibiting the texting of ePHI or limiting the type of information that may be shared via text message (e.g., limiting condition-specific information or information identifying a patient)
- Workforce training on the appropriate use of work-related texting
- Password protection and encryption for mobile devices that create, receive, or maintain text messages with ePHI
- An inventory of all mobile devices used for texting ePHI (whether provider-owned or personal devices)
- Proper sanitization of mobile devices that text ePHI upon retirement of the device
- A policy requiring annotation of the medical record with any ePHI that is received via text and is used to make a decision about a patient
- A policy setting forth a retention period or requiring immediate deletion of all texts that include ePHI
- Use of alternative technology, such as a vendor-supplied secure messaging application

Further Considerations for Compliant Texting

Providers may want to also consider whether any third party uses or discloses ePHI when texting occurs. With respect to telecommunications providers, the Department of Health and Human Services has stated that entities acting only as conduits of ePHI and that do not access the information other than on a random or infrequent basis as necessary for the performance of the transportation service do not qualify as business associates.[9]

In contrast, if texts are being stored indefinitely on a third party's server, such as when a text is sent to an e-mail account of a member of the workforce and the e-mail account is administered by a third party, then a business associate contract with the third party may be required.

Finally, providers may wish to address the use and disclosure of ePHI in their privacy policies and training and should consider sanctioning members of the workforce who violate such policies. Providers must also consider whether texts of PHI are subject to the HIPAA accounting of disclosures and, if so, whether they need to be included in a disclosure log.

There is no one-size-fits-all solution; different organizations may arrive at different conclusions regarding the threat posed by texting of PHI and what combination of controls reduces risks to a reasonable and appropriate level. There are some controls

that are simply not going to be available for traditional texting, such as centralized audit controls that allow the IT department to monitor texts containing PHI.

Each healthcare organization must decide whether it will prohibit or allow texting. This may be a fluid process, requiring the monitoring and reevaluation of policies to determine if they are effective. It is ultimately imperative to recognize both the value and risks of texting and to proactively address the issues.

Notes

1. comScore. "comScore Reports October 2011 U.S. Mobile Subscriber Market Share." Press release. December 2, 2011. www.comscore.com/Press_Events/Press_Releases/2011/12.
2. TigerText. "Physician and Hospital Texting Is on the Rise." Press release. October 12, 2011. www.tigertext.com/physician-texting-on-rise.
3. Borland, John. "Breaking GSM with a $15 Phone … Plus Smarts." *Wired*, December 28, 2010. www.wired.com/threatlevel/2010/12/breaking-gsm-with-a-15-phone-plus-smarts.
4. HIPAA, Public Law 104-191, 45 CFR §§ 164.524, 164.526.
5. HIPAA, 45 CFR § 164.501.
6. Office for Civil Rights, US Department of Health and Human Services. "Guidance on Risk Analysis." July 14, 2010. www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Note, while the guidance references that the data collection should address where ePHI is "stored, received, maintained, and transmitted," the use of "stored" is likely an error and should instead be "created" based on the phrase "created, received, maintained, and transmitted" appearing elsewhere in the same guidance.
7. "SMS." Wikipedia. http://en.wikipedia.org/wiki/SMS#Vulnerabilities.
8. Office for Civil Rights. "Guidance on Risk Analysis."
9. Office for Civil Rights. "Are the following entities considered 'business associates' under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management." March 14, 2006. www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/245.html.

Adam H. Greene (adamgreene@dwt.com) is a partner at Davis Wright Tremaine LLP.

Article citation:
Greene, Adam H. "HIPAA Compliance for Clinician Texting" *Journal of AHIMA* 83, no.4 (April 2012): 34-36.