Commentary on "Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance"

The article by Drolet et al,[1] which reviews the results of a survey of the American Society for Surgery of the Hand (ASSH) members regarding their use of text messaging to communicate protected health information (PHI), raises questions regarding physicians' obligations to maintain the privacy and security of PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA or the Act).

Since HIPAA's initial adoption, Congress and the U.S. Department of Health and Human Services (HHS) have modified the Act through regulations and amendments designed to protect patient privacy rights and establish the obligations of "covered entities"[2] including health care providers, health plans, and health care clearinghouses, and their "business associates,"[3] such as third-party administrators, accountants, transcriptionists, and billing personnel, to safeguard PHI. The most sweeping changes, however, occurred with the adoption of the HIPAA Omnibus Rule of 2013 (Omnibus Rule), through which HHS implemented statutory amendments under the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[4] Those amendments strengthened the protection of individuals' health information under the HIPAA Privacy and Security Rules, modified the HIPAA Enforcement Rules (to allow for increased and tiered civil monetary penalties), and amended the Breach Notification Rule to establish more objective standards for reporting breaches of unsecured PHI.[5] The Omnibus Rule also extended the applicability of certain Privacy and Security Rules' requirements to business associates, who had been involved in some of the largest breaches of PHI reported to HHS.[4] In effect, the Omnibus Rule transformed HIPAA into a law that not only greatly enhanced patient privacy rights but also bolstered the ability of the federal government to enforce those rights against health care providers and their business partners.[4]

For purposes of physician compliance, one should think of HIPAA in terms of the "suite" of regulations generated by the legislation: the Privacy Rule, the Security Rule, and the Breach Notification Rule. The Privacy Rule establishes national standards for the use and disclosure of PHI in any form: electronic, paper, or oral.[6] The Security Rule applies only to electronic PHI (ePHI). It establishes administrative, physical, and technical safeguards that covered entities and their business associates must put in place to safeguard the confidentiality, integrity, and availability of ePHI.[7] The Breach Notification Rule requires providers to notify affected individuals, including patients, HHS, and, in some cases, the media, of a breach of unsecured PHI.[6]

Each of the Rules addresses the use of electronically exchanged PHI, including text messaging, in patient care. For example, the HHS Office of Civil Rights (OCR), which is responsible for enforcing the Rules, has specifically announced (through a "Frequently Asked Questions" publication at hhs.gov) that the "Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so."[8] The OCR further suggests that health care providers should take steps to avoid unintentional disclosures, such as by sending e-mail alerts to patients to confirm their addresses prior to sending them messages and by limiting the amount and type of information disclosed through unencrypted e-mail.[9] Significantly, the guidance directs covered entities to ensure that any transmission of ePHI complies with the requirements of the Security Rule.[9]

The Security Rule includes both "Administrative Safeguards" and "Technical Safeguards" that establish important standards for health care providers managing and transmitting ePHI. For example, the Administrative Safeguards include a standard that requires covered entities to "implement policies and procedures to prevent, contain, and correct security violations."[10] Pursuant to that standard, providers must not only conduct a thorough assessment of the potential risks and vulnerabilities to the confidentiality of ePHI in their possession, or in the possession

◆ Published by Elsevier, Inc. All rights reserved. ◆

of a business associate, but also must "implement security measures sufficient to reduce the risks and vulnerabilities to reasonable and appropriate levels."[10] Thus, to comply with the Security Rule, health care providers using ePHI must undertake risk assessments and implement measures—albeit only those considered "reasonable and appropriate" under the circumstances—to reduce the possibility of a security breach. Industry experts characterize those requirements as representing the need for a proactive, rather than a reactive, approach to security.

In addition, the Security Rule includes a "Technical Safeguard" on transmission security, which includes a standard that requires health care providers to "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[11] Pursuant to the standard, health care providers must, among other things, encrypt ePHI "whenever appropriate."[11] This "transmission security" standard is the most directly applicable to providers' use of e-mail, text, and other mobile applications. It also begs the question as to what protections are "reasonable and appropriate" to implement before an individual provider transmits texts, taking into consideration the specific practice setting, the nature of the information being transmitted, the type of mobile device being used, and the application used for the transmission.

The utilization of mobile device applications has become so prevalent that HHS has issued fairly extensive guidance specifically addressing the transmission of ePHI (any use of mobile devices is by its nature electronic) through the use of laptops, tablets, and smartphones. Although its guidance appears to recognize the benefits of a mobile medical workforce, that is, one in which physicians can check patient records and test results from wherever they are, it also acknowledges that the increasing use of technology carries with it increased security risks.

In fact, HHS has devoted an entire page to "Your Mobile Device and Health Information and Security" on healthit.gov.[12] Among other things, it recommends the following 5 steps that a health care practice can take to manage use of its mobile devices: (1) understand the risks to the practice before electing to use mobile devices to access, receive, transmit, or store ePHI; (2) conduct a risk analysis to identify threats and vulnerabilities; (3) identify a mobile device risk management strategy, including safeguards; (4) develop, document, and implement mobile device policies and procedures to safeguard health information; and (5) conduct mobile device privacy and security awareness training for providers and professionals.

There is no question that the use of mobile devices to access, receive, transmit, or store ePHI carries privacy and security risks. Devices may be lost or stolen, or the user may inadvertently misdirect a message or download viruses or other malware that subject the device, and the data it stores, to a security breach. To the extent a mobile device with ePHI is used on an unsecure Wi-Fi network or shared with friends, family, or coworkers, its security may be compromised, and the ePHI may unintentionally be disclosed to unauthorized users.

To respond to those risks, healthit.gov recommends the following practices to protect and secure ePHI on mobile devices, including the provider's personal devices:

- Use complex passwords or other user identification
- Install and enable whole disk encryption
- Install and enable remote wiping and remote disabling features
- Disable and do not install or use file-sharing applications
- Install and enable a firewall
- Keep security software up to date
- Research mobile applications before downloading
- Maintain physical control of the device
- Use adequate security to send and receive health information over public Wi-Fi networks
- Delete all stored health information before discarding or reusing a mobile device[13]

Somewhat surprisingly, despite all the flexibility with which it generally approaches the use of mobile devices, HHS takes a relatively firmer line with respect to the use of text messaging to access, receive, transmit, and store ePHI. Specifically, HHS cites 3 reasons why it may not be appropriate to communicate ePHI by text, even to other providers: (1) text messages are generally not secure because they lack encryption; (2) the sender does not know with certainty whether the message is received by the intended recipient; and (3) the wireless carrier may store the text messages.[14] The HHS does acknowledge, however, that a provider's organization may approve texting after conducting a risk analysis or taking other measures to establish a secure communications platform for texting on mobile devices.[14]

Assuming the reliability of the survey results, a significant number of hand surgeons already use text messaging to communicate ePHI. Given the advantages that texting can provide (in terms of fast and easy access, receipt, and transmission), it is unlikely that they will abandon such use. Thus, they should address the use of mobile devices in their risk assessments and adopt policies that require training in the secure use of mobile devices and use of complex password protection, secure texting applications, and immediate deletion of ePHI texts. Although no one can ensure complete security under even the best circumstances, it is important for hand surgeons to demonstrate that they have taken steps to implement security measures and reduce risks and vulnerabilities to reasonable and appropriate levels.

*Susan Feingold Carlson**
*Jed R. Mandel**
**Chicago Law Partners, LLC, Chicago, IL*

http://dx.doi.org/10.1016/j.jhsa.2017.04.014

No benefits in any form have been received or will be received related directly or indirectly to the subject of this article.
The information provided in this article should not be construed as legal advice or a legal opinion. Consult a lawyer concerning your specific situation or legal questions.
Chicago Law Partners, LLC, serves as general counsel to the ASSH.

REFERENCES

1. Drolet BC, Marwaha JS, Hyatt B, Blazar PE, Lifchez SD. Electronic communication of protected health information: privacy, security, and HIPAA compliance. *J Hand Surg Am.* 2017;42(6):411−416.
2. U.S. Department of Health & Human Services. *HIPAA for Professionals: Covered Entities and Business Associates*. Available at: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html?language=en. Accessed April 27, 2017.
3. U.S. Department of Health & Human Services. *HIPAA for Professionals: Business Associates*. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es. Accessed April 27, 2017.
4. U.S. Department of Health & Human Services. *New Rule Protects Patient Privacy, Secures Health Information*. Available at: http://web.archive.org/web/20130201080317/http://www.hhs.gov/news/press/2013pres/01/20130117b.html. Updated January 17, 2013. Accessed April 27, 2017.
5. U.S. Department of Health & Human Services. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. *Fed Regist.* 2013;78(17):5565−5702.
6. U.S. Department of Health & Human Services. *HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules.* Available at: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf. Updated August 2016. Accessed April 27, 2017.
7. The Office of the National Coordinator for Health Information Technology. *Guide to Privacy and Security of Electronic Health Information*. Version 2.0. Available at: https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Updated April 2015. Accessed April 27, 2017.
8. U.S. Department of Health & Human Services. *HIPAA for Professionals: Does the HIPAA Privacy Rule Permit a Covered Health Care Provider to E-Mail or Otherwise Electronically Exchange Protected Health Information (PHI) With Another Provider for Treatment Purposes?* Available at: https://www.hhs.gov/hipaa/for-professionals/faq/568/does-hipaa-permit-a-covered-health-care-to-email-information-with-another-provider/index.html. Updated December 15, 2008. Accessed April 27, 2017.
9. U.S. Department of Health & Human Services. *HIPAA for Professionals: Does the HIPAA Privacy Rule Permit Health Care Providers to Use E-Mail to Discuss Health Issues and Treatment With Their Patients?* Available at: https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html. Updated December 15, 2008. Accessed April 27, 2017.
10. Office of the Federal Register National Archives and Records Administration. *HIPAA Security Rule* § *164.308(a)(1)*. Available at: https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1.pdf. Updated October 1, 2007. Accessed April 27, 2017.
11. Office of the Federal Register National Archives and Records Administration. *HIPAA Security Rule* § *164.312(e)(1)*. Available at: https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1.pdf. Updated October 1, 2007. Accessed April 27, 2017.
12. The Office of the National Coordinator for Health Information Technology. Your Mobile Device and Health Information Privacy and Security. Available at: https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security. Updated March 21, 2014. Accessed April 27, 2017.
13. The Office of the National Coordinator for Health Information Technology. *How Can You Protect and Secure Health Information When Using a Mobile Device?* Available at: https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device. Updated January 24, 2013. Accessed April 27, 2017.
14. The Office of the National Coordinator for Health Information Technology. *Can You Use Texting to Communicate Health Information, Even If It Is to Another Provider or Professional?* Available at: https://www.healthit.gov/providers-professionals/frequently-asked-questions/533#id210. Updated January 15, 2013. Accessed April 27, 2017.