EDITOR'S CHOICE

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

Brian C. Drolet, MD,* Jayson S. Marwaha, BS,† Brad Hyatt, MD,‡
Phillip E. Blazar, MD,§ Scott D. Lifchez, MD||

Purpose Technology has enhanced modern health care delivery, particularly through accessibility to health information and ease of communication with tools like mobile device messaging (texting). However, text messaging has created new risks for breach of protected health information (PHI). In the current study, we sought to evaluate hand surgeons' knowledge and compliance with privacy and security standards for electronic communication by text message.

Methods A cross-sectional survey of the American Society for Surgery of the Hand membership was conducted in March and April 2016. Descriptive and inferential statistical analyses were performed of composite results as well as relevant subgroup analyses.

Results A total of 409 responses were obtained (11% response rate). Although 63% of surgeons reported that they believe that text messaging does not meet Health Insurance Portability and Accountability Act of 1996 security standards, only 37% reported they do not use text messages to communicate PHI. Younger surgeons and respondents who believed that their texting was compliant were statistically significantly more like to report messaging of PHI (odds ratio, 1.59 and 1.22, respectively).

Discussion A majority of hand surgeons in this study reported the use of text messaging to communicate PHI. Of note, neither the Health Insurance Portability and Accountability Act of 1996 statute nor US Department of Health and Human Services specifically prohibits this form of electronic communication. To be compliant, surgeons, practices, and institutions need to take reasonable security precautions to prevent breach of privacy with electronic communication.

Clinical relevance Communication of clinical information by text message is not prohibited under Health Insurance Portability and Accountability Act of 1996, but surgeons should use appropriate safeguards to prevent breach when using this form of communication. *(J Hand Surg Am. 2017;42(6):411–416. Copyright © 2017 by the American Society for Surgery of the Hand. All rights reserved.)*

Key words Electronic communication, protected health information, HIPAA, ethics, professionalism.

*From the *Department of Plastic Surgery, Department of Biomedical Informatics, Center for Biomedical Ethics and Society, Vanderbilt University Medical Center, Nashville, TN; the †Warren Alpert Medical School of Brown University, Providence, RI; the ‡Department of Orthopedic Surgery, San Antonio Military Medical Center, San Antonio, TX; the §Department of Orthopedic Surgery, Brigham and Women's Hospital, Boston, MA; and the ||Department of Plastic and Reconstructive Surgery, Johns Hopkins Medicine, Baltimore, MD.*

Received for publication July 12, 2016; accepted in revised form March 19, 2017.

No benefits in any form have been received or will be received related directly or indirectly to the subject of this article.

Corresponding author: Brian C. Drolet, MD, Department of Plastic Surgery, Medical Center North, D-4219 Nashville, TN 37232; e-mail: brian.c.drolet@gmail.com.

0363-5023/17/4206-0001$36.00/0
http://dx.doi.org/10.1016/j.jhsa.2017.03.023

Technology and electronic communication are both widespread and essential in modern health care delivery. Patients now have remote access to their health records and providers through electronic medical record portals and other electronic modalities.[1,2] Likewise, health care providers can more rapidly communicate with each other and patients, particularly in the form of email and short message service or "text" communication.[3,4]

Recent surveys have found that more than half of physicians use text messaging to communicate with colleagues about patient care. These studies have found that 2-way text communication offers several advantages to traditional 1-way paging systems including convenience and reliability.[5–8]

This open exchange of information among providers and with patients has the potential to improve health care access, patient understanding, and even health outcomes.[9–12] However, health information is both sensitive and protected under law. Therefore, care must be taken any time such information is communicated or transmitted, regardless of the form (ie, verbal, written, or electronic). To ensure the protection of health information, nearly all developed countries have laws dictating standards for privacy and security. In the United States, Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides the basis for federal regulations, as amended pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 (collectively referred to as HIPAA).

According to HIPAA, information related to an individual's past, present, or future physical or mental conditions is considered protected health information (PHI). Under the minimum necessary requirement, health care providers and facilities must take "reasonable steps to limit the use or disclosure of [PHI] to the minimum necessary to accomplish the intended healthcare purpose."[13] Additionally, Privacy and Security Rules require that health care staff and facilities implement "appropriate administrative, technical and physical safeguards" to prevent breach of PHI.[14,15]

Breach of PHI is defined explicitly as "the acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual."[16] Breach is a major concern, particularly with the communication of unsecured electronic PHI, which can be copied, shared, misdirected (such as by accidental transposition of digits of a phone number when texting), or transmitted to anywhere or anyone in the world.

To deter breach, there are considerable penalties for impermissible use or improper disclosure of PHI.[14,15] One of the major provisions of the US Department of Health and Human Services (HHS) Health Information Technology for Economic and Clinical Health Act of 2009 includes penalties for HIPAA violations (Table 1).[17]

TABLE 1. Range of Monetary Penalties That Can Be Assessed to Providers for HIPAA Violation(S) Depending on Frequency and Presence/Absence of Adequate Protections in Place at the Time of the Violation

Violation Category	Individual Fine
Unknowing	$100–$50,000
Reasonable cause	$1,000–$50,000
Willful neglect—corrected	$10,000–$50,000
Willful neglect—not corrected	At least $50,000

Although there are concerns for maintaining "appropriate safeguards" on personal mobile text messaging, there are no federal regulations or HHS standards that prohibit the use of this technology[18] (Fig. 1). Yet, increasing regulation (eg, Health Information Technology for Economic and Clinical Health Act) and ambiguity in published guidance from HHS has led to uncertainty and frustration among clinicians.[19,20] Limited studies have examined text messaging among physicians, and the prevalence of text messaging by hand surgeons is unknown.[5,21–22] To examine this issue, the Ethics and Professionalism Committee of the American Society for Surgery of the Hand (ASSH) sought to learn more about hand surgeons' use and understanding of text messaging as well as HIPAA privacy and security compliance.

METHODS

After approval by our institutional review board, we developed and piloted a survey to evaluate electronic communication, as well as knowledge and understanding of HIPAA security and privacy rules, particularly relating to text messaging. The survey was piloted with a group of hand surgeons at the authors' local institutions, and revisions were made for content and clarity.

The survey was then distributed to the membership of the ASSH between March and April 2016. To maximize response, the survey was distributed on 6 separate occasions including by email, as well as inclusion in ASSH Current, and ASSH weekly member updates.

For our analysis, we studied ordinal scale responses. Two-sided confidence intervals were calculated for the proportion of respondents in each group using the