Clarifying the Confusion about HIPAA-Compliant Texting

May 2013

Authors:

Megan Hardiman
Partner
KattenMuchinRosenman LLP

Terry Edwards
President & CEO
PerfectServe, Inc.

Katten
Katten Muchin Rosenman LLP

perfectserve®

Table of Contents

Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

Introduction

In today's enhanced HIPAA enforcement environment, addressing information security is a top-of-mind concern for many health care leaders. The growing use of mobile devices in the health care industry makes HIPAA compliance both more challenging and more important than ever. Loss or theft of a mobile device containing unsecured protected health information (PHI) has been a source of numerous reported breaches and enforcement actions. The government's posting in late 2012 of an online educational initiative on protecting and securing mobile devices clearly underscores the need for leaders to carefully review existing practices and policies surrounding use of mobile devices, such as smartphones, tablets and laptops.[1]

Use of mobile devices for texting PHI presents a number of risks. The purpose of this paper is to examine the issues related to HIPAA compliance in the context of texting and to help health care leaders understand the risks and potential ways they can manage those risks.

The Burgeoning Growth of Electronic Communication[i]

In 2012, approximately 184.3 billion text messages were sent in the US each month, an increase from 28.9 billion a month just five years before.[2] The health care environment is not immune to the rapid growth in the use of electronic communication.

In fact, technology-enabling communication that is rapid and asynchronous (i.e., not requiring participants to communicate concurrently) holds many advantages in the fast-paced world of health care delivery. Increasingly, physicians and other health care providers are exchanging clinical information through text, or SMS (short message service), messages sent via smart phones or alpha numeric pagers, computerized physician order entry (CPOE), email and messaging features within the electronic medical record (EMR). A recent survey found that more than half of the 107 responding pediatric hospitalists used text messaging to communicate work-related information.[3]

Texting can be an efficient means of communication for busy providers. However, texting PHI without adequate safeguards can expose an organization to potential privacy and security violations that may result in breaches, adverse legal and financial consequences, as well as loss of patient trust and reputation in the marketplace. An organization needs to consider whether its policies and procedures sufficiently address texting PHI, and whether the workforce has been adequately trained to comply with those policies and procedures.

Texting In a Health Care Context

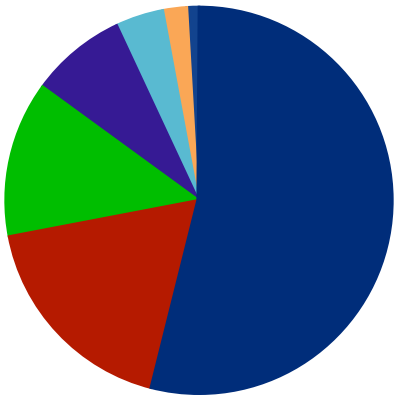
Text messages are commonly sent between two individuals via their respective mobile phones. However, health care providers may use other mechanisms to transmit text messages (see sidebar). For example, a nurse might create a message by logging onto the website of a mobile carrier. The message may be sent via the mobile carrier's network to a pager or via SMS to a physician's mobile phone. A pharmacist might telephone a call center with a message for a physician; the call center agent may create an electronic text message that is then sent to the physician via a mobile carrier's network or routed through the Internet. Text messages may be stored on mobile devices, workstations and telecommunication vendor/wireless carrier servers.

Texting Is Just One Piece of the Puzzle

Texting is more than simply sending messages from one mobile device to another. It also includes sending messages from mobile carrier web sites, web-based paging applications, call centers, answering services and hospital switchboards.

As illustrated in the chart below, health care providers at a 364-bed hospital generate approximately 200,000 outbound communications to physicians annually. Those communications follow different processes and include multiple contact modalities (e.g., voice calls, secure voice and text messages, SMS text message and alpha and numeric pages).

SMS text is just one piece of the communications puzzle at this 364-Bed Hospital.



Understanding HIPAA and Its Revisions

Enacted in 1996, HIPAA requires the Department of Health and Human Services (HHS) to create standards for the use and disclosure of protected health information and addresses the security and privacy of such information.[4,5] The HIPAA provisions were amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Among other changes, HITECH extended direct liability for HIPAA violations to business associates, dramatically strengthened the penalties for HIPAA violations and made a number of other changes to enhance the enforcement environment.

The final HIPAA omnibus rule (Final Rule), released in mid-January by the HHS Office for Civil Rights (OCR), implements many of the HITECH provisions and clarifies some elements of the original HIPAA legislation. The Final Rule became effective March 26, 2013; the general compliance deadline is September 23, 2013.

While HITECH put in place federal breach notification requirements for breaches of unsecured PHI, the Final Rule significantly revised the standard for notification. Prior to the Final Rule, notification was required only if the breach created a significant risk of harm to the individual. Under the Final Rule, there is a presumption in favor of notification, and a covered entity (CE) is generally required to provide notification for any breach of unsecured PHI, unless the organization demonstrates through a risk assessment a "low probability that has been compromised." Despite some ambiguities, it is widely anticipated that this revised standard will result in more notifications. (See sidebar for key definitions used in HIPAA.)

The HIPAA Security Rule regulates the security of ePHI. Generally, the Security Rule require CEs and their business associates to implement appropriate physical, administrative and technical safeguards to ensure the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits. [45 CFR 164.306(a).] Examples of administrative safeguards include conducting risk analyses and staff training. Ensuring a locked location for network servers

and shielding screens from unauthorized viewers are examples of physical safeguards. Technical safeguards include encryption and the use of secure passwords.

There Is No Such Thing as a HIPAA-Compliant Application or Device

The HIPAA Security Rule is "technology neutral." Furthermore, compliance with the HIPAA Security Rule is not an attribute of a particular application or device, but rather of a system of physical, administrative and technology safeguards that support the HIPAA-compliant use of electronic communication. Thus, there is no such thing as a "HIPAA-compliant" application or device.

HIPAA does not expressly require the use or avoidance of any specific modes of communication. Thus, HIPAA does not expressly prohibit (or even mention) texting.

Rather, as with any other means of communication, appropriate safeguards must be in place to ensure the privacy and security of PHI communicated by text. These safeguards must adequately address the specific risks that texting raises. For example, mobile device-to-mobile device SMS text messages are generally not secure because they lack encryption. Also, the sender does not know with certainty that his or her message is indeed received by the intended recipient. Furthermore, the telecommunications vendor/wireless carrier may store the text messages.

Recent HHS guidance indicates text messaging, as a means of communicating PHI, can be permissible under HIPAA, depending in large part on the adequacy of the controls used. Therein lies the rub. (For more information, see "Can you use texting to communication health information, even if it is to another provider or professional?" at http://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p).

Key Definitions within HIPAA

Three of the most important terms defined within HIPAA are protected health information, covered entity and business associate.[6] Protected health information (PHI) is broadly defined by HIPAA, and generally includes even basic demographic information held by a covered entity as a result of the provision of health care, or payment for health care. The term "covered entity" (CE) generally includes health plans, most health care providers and health care clearinghouses. A "business associate" (BA) is an entity that performs a function or activity involving PHI on behalf of a CE, such as billing, answering service, transcription, record storage or shredding services. CEs are required to obtain business associate agreements with all BAs, specifying the privacy and security requirements for the BA's use and disclosure of PHI.

A Worst Case Scenario: Security Breaches

Compliance with HIPAA has never been more important (see Table 1). Since HITECH, OCR has issued the first civil monetary penalty for a HIPAA violation, entered into a number of significant resolution or settlement agreements for alleged HIPAA violations, and begun the roll-out of a pilot HIPAA audit program. Since 2003, the OCR has investigated more than 77,000 complaints of HIPAA violations and has required corrective action in more than 18,000.[7]

One of the most frequent compliance issues has been lack of administrative safeguards of ePHI. During first three years after the compliance deadline for public reporting of PHI security breaches affecting more than 500 individuals, the OCR received reports of almost 490 such events.[8] These breaches affected

the PHI of more than 21 million individuals. Just over half of the events were the result of theft. Another 20 percent were due to unauthorized access or disclosure. Thousands of breaches affecting fewer than 500 people also occurred.

In a 2012 study by the Ponemon Institute, 94 percent of the 80 CEs surveyed reported at least one data breach in the past two years.[9] Almost half reported more than five incidents, up from 29 percent in 2010. The most common cause of these breaches was loss or theft of a computing device (46 percent).

Data breaches involving PHI can be expensive. In addition to the costs of investigation, notification and mitigation, they can result in litigation, expensive settlements and corrective action plans, or other enforcement, including potential civil monetary penalties.

In 2012, the Massachusetts Eye and Ear Infirmary (MEEI) reached a $1.5 million agreement with HHS and agreed to a 3-year corrective action plan after an employee's laptop containing unencrypted PHI was stolen.[10] Notably, OCR's investigation followed a breach report submitted by MEEI. In another case, Blue Cross/Blue Shield of Tennessee reached a $1.5 million agreement with HHS after 57 unencrypted computer hard drives containing PHI of more than one million individuals were stolen from a leased facility. Reportedly, the health insurer also incurred more than $17 million in direct expenses related to the investigation and remediation of the incident.

In the study conducted by the Ponemon Institute, the average cost of data breaches during the previous two years was $2.4 million per organization.[9]

Table 1: Categories of HIPAA Violations and Penalty Amounts

Violation category	Penalty for each violation	Penalty for all such identical violations in a calendar year
Did not know	$100 - $50,000	$1,500,000
Reasonable cause	$1,000 - $50,000	$1,500,000
Willful neglect, corrected	$10,000 - $50,000	$1,500,000
Willful neglect, not corrected	$50,000	$1,500,000

Source: Department of Health and Human Services. Federal Register. 2013; 78(17):5583

While federal agencies are the primary enforcement agencies, under changes made by HITECH, state attorney generals were also given authority to enforce HIPAA violations in certain circumstances. State attorneys general may also bring actions under a variety of state laws. For example, some states have adopted sweeping privacy laws with significant penalties[ii], and most states have data breach notification statutes that apply to PHI. In recent years, state attorneys general have actively investigated potential breaches.

Managing Mobile Devices in Your Health Care Organization

Key steps organizations can take to manage mobile devices used by health care providers include:

1. Decide whether mobile devices will be used to access, receive, transmit or store patients' health information or will be used as part of your organization's internal network or systems, such as an electronic health record system.
2. Consider the risks when using mobile devices to transmit the health information your organization holds.
3. Identify a mobile device risk management strategy, including privacy and security safeguards.
4. Develop, document and implement your organization's mobile device policies and procedures to safeguard health information.
5. Conduct mobile device privacy and security awareness and ongoing training for providers and professionals.

Source: Department of Health and Human Services. Managing mobile devices in your health care organization. Available at: http://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf. Accessed April 9, 2013.

For example, in 2012, South Shore Hospital reached a settlement with the Massachusetts attorney general's office for violation of federal HIPAA provisions and state consumer protection laws.[11] The hospital agreed to pay $750,000 and implement extensive corrective action after two boxes of unencrypted backup tapes containing PHI of more than 800,000 individuals were lost during shipment to an off-site facility.

State attorneys general have also brought action against business associates for alleged violations of HIPAA and state law, as in the case of the Minnesota attorney general's action against Accretive Health.[12]

These and other highly visible cases underscore the potential consequences of PHI breaches in cost and organizational reputation in the marketplace—and emphasize the importance of a proactive risk management strategy.

Managing Risk Effectively

So, can you use texting to communicate health information, even if it is to another provider or professional? In the frequently asked questions section of its Mobile Device Guidance, HHS answers, "It depends." After summarizing some of the key risks of texting PHI, HHS states that:

However, your organization may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices.

For more information, see the sidebar and "Can you use texting to communicate health information, even if it is to another provider or professional?" at http://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p.

Evaluating Texting Risks as Part of the Organization's Risk Analysis

Organizations should evaluate whether to permit texting as part of a thorough risk analysis.

A HIPAA risk analysis is the foundation for safeguarding electronic PHI, and leads to an overall risk management strategy.[13] The HIPAA rules do not mandate a "one size fits all" approach to risk analysis.[14] Methods will vary dependent on the size, complexity and capabilities of the organization; however, all affected organizations, regardless of size, are expected to conduct an appropriate risk analysis. Failure to do so is frequently cited as an alleged violation in OCR settlements, and small organizations are not exempt from this requirement.

The following questions adapted from NIST Special Publication (SP) 800-665 are examples organizations could consider as part of a risk analysis.

- Has the organization identified the ePHI within the organization? This includes ePHI that the organization creates, receives, maintains or transmits.

- What are the external/third party sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI?

- What are the human, natural and environmental threats to information system that contain ePHI?

The risk analysis should identify threats and vulnerabilities to ePHI, assess the sufficiency of current security measures, determine the likelihood and potential impact of threat occurrence, assign levels of risk to these threats and identify and implement appropriate corrective actions.

With regard to texting, key risks include the risk of loss, theft or improper disposal of the mobile device containing unsecured PHI and the risk that individuals other than the intended recipient may gain access to PHI stored in texts as a result of lack of safeguards (for example, someone who steals the phone, or a family member who borrows the phone).

Another possible risk is that, while in transit, PHI could be intercepted by unauthorized persons. Also, telecommunications vendors or wireless carriers that store texts containing PHI may need to execute business associate agreements.

Managing Texting Risks as Part of the Overall Risk Management Strategy

After analyzing the risks, some organizations may decide to ban texting of PHI, while others may decide to approve texting only after implementing appropriate security measures. Based on its risk analysis, an organization must develop a risk management plan that addresses its needs and vulnerabilities, and that manages its anticipated risks to a reasonable and appropriate level.

A 2012 article in the Journal of AHIMA listed some examples of safeguards that may form part of a risk management plan:

- Banning the texting of ePHI entirely, or limiting the texting of identifiers, diagnosis and other information

- Requiring deletion of texts (policies also need to address circumstances where HIPAA requires ePHI in texts be included in the medical record to address individual patient rights)
- Passcode protection
- Encryption (see sidebar)
- Secure disposal of devices (see sidebar)
- Registration of devices, including personally-owned devices
- Use of a third-party secure messaging solution[15]

Regular training on the CE's policies and procedures is essential to promoting organization-wide compliance and minimizing risk. As regards texting, it is critical that a workforce clearly understands the organization's policy and receives the training necessary for compliance. A substantial proportion of reported security breaches are due in part to insufficient training of workforce. It is also important that there be sanctions for non-compliance.

Risk management is a process. To ensure continued compliance with security standards, organizations must conduct ongoing monitoring of their information security risk to determine whether it is being effectively managed by existing safeguards, or whether those safeguards need to be strengthened. Changes in the regulatory environment, such as enforcement actions or the issuance of additional guidance, also need to be monitored. Leaders should also ensure the risk analysis is updated regularly as technology and health care delivery change —for example, in response to the greater care coordination required with accountable care.

Conclusion

Compliance with the HIPAA Security Rule is not an attribute of a particular application or device, but rather of a system of physical, administrative and technology safeguards that support the HIPAA-compliant use of electronic communication. Texting can be a useful means of communication, but texting PHI presents a number of risks. Organizations must thoroughly analyze these risks and develop appropriate policies. Where an organization decides to permit texting, it is essential that the associated privacy and security risks are effectively managed.

Resources for Encryption and Sanitation Requirements

Encryption, which must be addressed as part of an organization's HIPAA security compliance, can be used to secure data in transmission (such as PHI sent by a mobile device) and data at rest (such as PHI stored locally on a mobile device). OCR guidance describes the requirements for encryption for data at rest and data in motion which, if employed, will create a safe harbor from the need for breach notification if the data is lost or stolen.

For encryption of data at rest, see National Institute of Standards and Technology (NIST) Special Publication 800-111.

For encryption of data in motion, see NIST Special Publication 800-77, and the OCR guidance mentioned below.

For sanitation of electronic media, see NIST Special Publication 800-88.

For further information, see OCR guidance at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[i] While this article focuses only on HIPAA risks, organizations accredited by The Joint Commission will also want to review and consider The Joint Commission's Standards FAQ on Texting Orders, which states that "it is not acceptable for physicians or other licensed independent practitioners to text orders for patients to the hospital or other healthcare setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record." See, http://www.jointcommission.org/mobile/standards_information/jcfaqdetails.aspx?StandardsFAQId=401&StandardsFAQChapterId=79.

[ii] See, for example, the Texas Medical Records Privacy Act, Texas Health & Safety Code, Chapter 181.

About The Authors

Megan Hardiman
Partner
KattenMuchinRosenman LLP

Megan Hardiman draws on her broad regulatory background to advise clients on Stark Law and Anti-Kickback Statute compliance matters, state fee-splitting and corporate practice of medicine prohibitions, tax exemption issues and corporate governance matters. She also has significant depth in the area of health information privacy and security, including HIPAA and the HITECH Act.

Ms. Hardiman's transactional experience includes sales, acquisitions and affiliations involving a wide variety of health care industry clients, such as hospitals and health systems, home infusion companies, senior housing providers, urgent care centers and medical colleges. She has represented tax-exempt health systems in structuring numerous complex joint operating agreements and affiliations with unrelated health systems, and has obtained favorable rulings from the Internal Revenue Service on the consequences of these and other transactions among tax-exempt organizations.

Ms. Hardiman received her BS in journalism, with high honors, from the University of Illinois and her JD, cum laude, from the University of Illinois College of Law. Ms. Hardiman has written articles for the American Health Lawyers Association and other industry publications.

Terry Edwards
President &CEO
PerfectServe, Inc.

Terry Edwards is the founding CEO and visionary behind PerfectServe's industry-leading clinical communication and information delivery platform. Starting in 1997, Edwards invented and developed PerfectServe's original voice interfaces and rules-based communications routing applications. Since that time, he has successfully guided the company's national expansion to more than 30,000 physicians in 10,000 practices and more than 60 hospitals.

PerfectServe enables more accurate, reliable and secure clinical communications. Its cloud-based applications and platform help hospitals and health systems implement HIPAA-compliant communication processes while improving operating efficiencies and the quality of care. With PerfectServe, clinicians are able to communicate with each other more easily across the care continuum.

References

1. Department of Health and Human Services. Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security of Health Information. *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*. Available at: www.HealthIT.gov/mobiledevices. Accessed April 24, 2013.

2. CTIA. Wireless quick facts. 2012. Available at: http://www.ctia.org/advocacy/research/index.cfm/aid/10323. Accessed February 27, 2013.

3. Kuhlmann S, Ahlers-Schmidt CR, Steinberger E. Text messaging as a means of communication among pediatric hospitalists. 2012. Abstract presented at American Academy of Pediatrics National Conference. October 21, 2012. New Orleans. Available at: https://aap.confex.com/aap/2012/webprogrampress/Paper17820.html. Accessed February 27, 2013.

4. Department of Health and Human Services. HIPAA administrative simplification statute and rules. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html. Accessed March 5, 2013.

5. American Medical Association. HIPAA: Health Insurance Portability and Accountability Act. Available at: http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page. Accessed November 5, 2012.

6. Department of Health and Human Services. Summary of the HIPAA privacy rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Accessed March 5, 2013.

7. Department of Health and Human Services. Enforcement highlights. January 2013. Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html. Accessed February 28, 2013.

8. American Health Information Management Association. CR reports over 21 million impacted by large-scale breaches. 2012. Available at: http://journal.ahima.org/2012/09/12/three-years-later-ocr-reports-over-21-million-impacted-by-large-scale-breaches. Accessed February 28, 2013.

9. Ponemon Institute. Third annual benchmark study on patient privacy & data security. 2012. Available at: http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf. Accessed February 28, 2013.

10. Department of Health and Human Services. Massachusetts provider settles HIPAA case for $1.5 million. Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html. Accessed March 5, 2013.

11. Attorney General of Massachusetts. South Shore Hospital to pay $750,000 to settle data breach allegations. [press release] Available at: http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html. Accessed March 5, 2013.

12. Office of the Minnesota Attorney General. Available at: http://www.ag.state.mn.us/Consumer/PressRelease/07312012AccretiveCeaseOperations.asp. Accessed April 24, 2013.

13. Department of Health and Human Services. Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security of Health Information. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed January 9, 2013.

14. Department of Health and Human Services. Guidance on risk analysis requirements under the HIPAA security rule. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed April 24, 2013.

15. Greene AH. HIPAA Compliance for clinician texting. *J AHIMA*. 2012; 83(4): 34-36.