Maintaining HIPAA Compliance in a Mobile World

Introduction

We live in an era of mobile communication and text messaging. Mobile phone adoption is nearly ubiquitous, with wireless devices now outnumbering people in the United States. Text messaging (SMS, IP/Push Notifications, Group Chat) represents an increasingly popular form of communication, and many people now prefer text messaging to traditional phone calls.

This rapid shift toward mobile, text-based communication has profound implications for the healthcare industry. Text messaging can circumvent the inefficiencies of pagers and other legacy systems, dramatically improving workflows through faster and more effective communication. Application features like image sharing and group chats can create additional benefits.

The growing use of mobile devices in the healthcare industry makes HIPAA compliance more challenging and more important than ever. Standard text messaging on most devices is not secure and fails to comply with HIPAA standards. Furthermore, loss or theft of a mobile device containing unsecure protected health information has been a source of numerous reported breaches and enforcement actions.

The purpose of this whitepaper is to discuss challenges to HIPAA in the context of the rapidly growing use of mobile messaging within the healthcare industry.

Understanding HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA is divided into three different titles or sections that address a unique aspect of health insurance reform. Two main sections deal with Portability and Administrative Simplification; the third and last section deals with Privacy.

In a nutshell, HIPPA:

- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
- Reduces health care fraud and abuse;
- Mandates industry-wide standards for health care information on electronic billing and other processes; and

- Requires the protection and confidential handling of protected health information

This whitepaper will focus on privacy. Specifically, HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared.

HIPAA provides for the protection of individually identifiable health information that is transmitted or maintained in any form or medium. The privacy rules affect the day-to-day business operations of all organizations that provide medical care and maintain personal health information.

HIPAA protects an individual's health information and his/her demographic information. This is called "protected health information" or "PHI". Information meets the definition of PHI if, even without the patient's name, if you look at certain information and you can tell who the person is then it is PHI. The PHI can relate to past, present or future physical or mental health of the individual. PHI describes a disease, diagnosis, procedure, prognosis, or condition of the individual and can exist in any medium – files, voice mail, email, fax, verbal communications, as well as mobile communications, including text messages.

HIPAA defines information as protected health information if it contains the following information about the patient, the patient's household members, or the patient's employers:

- Names
- Dates relating to a patient , i.e. birthdates, dates of medical treatment, admission and discharge dates, and dates of death
- Telephone numbers, addresses (including city, county, or zip code) fax numbers and other contact information
- Social Security numbers
- Medical records numbers
- Photographs
- Finger and voice prints
- Any other unique identifying number

HIPAA requires the following "covered entities" (CE) to comply:

Health Care Providers: Any provider of medical or other health Services that bills or is paid for healthcare in the normal course of business. Health care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, services, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual.

Health Plans: Individuals or group plans that provide or pay the cost of medical care and includes both Medicare and Medicaid programs.

Health Care Clearinghouse or Business Associate (BA): Businesses that process or facilitate the processing of health information, including billing, answering service, transcription, record storage or shredding services. CEs are required to obtain agreements with all BAs, specifying the privacy and security requirements for the BA's use and disclosure of PHI.

The Importance of HIPAA Compliancy in a Mobile World

In 2013, 19.5 billion SMS text messages were sent daily, and the number of IP/ Push Notifications sent daily doubled to 41 billion.[1] There is no denying the rapid growth of mobile communications and its impact on the healthcare environment. In fact, a new survey of pediatric hospitalists finds that 57% of clinicians send work-related text messages.[2] Furthermore, 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.

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. Texting can be an efficient means of communication for busy providers.

However, texting protected health information without the necessary safeguards poses a major risk for healthcare providers and organizations and can lead to potential privacy and security violations, adverse legal and financial consequences, as well as a loss of patient trust and reputation in the marketplace.

For example, imagine a scenario in which health care providers regularly text message each other protected health information, including clinical information and patient prescriptions. Text messages may reside on a mobile device indefinitely, which means patient information could be subject to theft or loss, or could be viewed by unauthorized persons. Also, texts are not subject to central monitoring by the IT department and can be easily intercepted. Finally, the HIPAA privacy rule requires that if text messages are used to make medical decisions, patients should have the right to access and amend that information. So texts that aren't documented in EHRs could be a HIPAA violation.

Healthcare organizations need to address the technology aspect of texting and put in place policies and procedures to address the security and privacy risks to ensure HIPAA compliancy. HIPAA does not expressly require the use or avoidance of any specific

[1] http://www.digitaltrends.com/mobile/chat-apps-to-double-sms-traffic-by-end-of-2013/#ixzz3JzUPeG6m

[2] http://www.informationweek.com/mobile/text-messaging-between-clinicians-increasing-in-hospitals/d/d-id/1107145

modes of communication, including texting. Rather, as with any means of communication, appropriate safeguards must be in place to ensure the privacy and security of PHI communicated by text.

Mitigating the Risks of Mobile Messaging PHI

A HIPAA risk analysis is the foundation for safeguarding electronic PHI, and leads to an overall risk management strategy. The use of mobile communications including texting also needs to be evaluated as part of the HIPAA risk analysis.

Organizations can take to manage mobile devices used by health care providers include:

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

Furthermore, the following safeguards can be incorporated to mitigate texting risks and comply with HIPAA:

- Deletion of texts from mobile devices after a certain period of time
- Passcode protection
- Encryption
- Secure disposal of devices
- Registration of devices, including personally owned devices
- Use of a third-party messaging solution

The HIPAA Security Rule is "technology neutral." Compliance with HIPAA is not an attribute of a particular application or device, but rather a system of administrative, physical and technical safeguards that support HIPAA.

Conclusion

Mobile communications will continue to grow, and especially within the healthcare industry. Mobile messaging is a useful way to communicate PHI, but most consumer-grade text messaging falls short on all security and regulatory compliance requirements. One solution is the implementation of enterprise mobile messaging platforms that allow health care enterprises to utilize mobile technology to increase efficiency, improve patient care, and drive new business without compromising on HIPAA compliance standards.

Company Profile

TeleMessage provides HIPAA mobile messaging products. Our solution keeps information secure, ensures reliability, allows for management and administration of messages and increased productivity and efficiency.

The TeleMessage enterprise mobile messaging platform is:

Secure – with TeleMessage, messages and chat conversations are encrypted and password protected. We offer end-to-end encryption, password protection, time-limited messages, forward-locking, remote auto lock and wipe in case of theft or lost mobile devices, and advanced delivery confirmations.

Managed – TeleMessage allows you to administer, control, and enforce messaging & information transfer policies. The system includes an administrator interface, message archive, report generator and integrated company address book.

Reliable – TeleMessage makes sure that messages are received by the intended recipient worry-free. All IP Push Notifications that are not received within in a timely manner can be sent as a standard SMS message. We've also invested in our carrier-grade infrastructure, cross-carrier and cross-device message transmission, and emergency notification alert systems. We guarantee 99.95% SLA uptime.

IT-Ready – we've developed a range of APIs that can connect TeleMessage to any IT system in order to send messages, including REST, SOAP, XML, HTTP, and more. You can find all of our API documentation and developer resources on our Developer's Zone.

The solution includes a web portal, Android/iOS mobile apps, and Outlook Plug-In to send IP Push Notifications, SMS, voice, fax and email messages.

TeleMessage has been providing state-of-the-art messaging solutions since 1999. Our software has been successfully deployed and used by thousands of enterprises, trusted by dozens of telecom operators, reaches hundreds of millions of users and powers billions of messages through customers' networks. We support an ever growing number of enterprises, including leading brands across a range of industries such as healthcare, travel, finance and retail, among others.

TeleMessage is a fully owned subsidiary of Messaging International Plc, a publicly traded company on the London Stock Exchange under the symbol "MES".

Contact Us

To learn more about our HIPAA messaging platform, please contact us:
Tel: +1 (978) 263-1015 | Email: sales@TeleMessage.com