The Digitalization of Healthcare Communication

Prepared by:
Phil C. Solomon
MiraMed Global Services

LORMAN

March 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 700 available
- ☑ **Slide Decks -** More than 1700 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

The Digitalization of Healthcare Communication

- Phil C. Solomon

The Rise of Text Messaging in America

In 1934 marked a turning point for the great depression in America with unemployment decreasing to 22 percent. This period was difficult even for those who did have jobs. An American worker's average wages were just $1,600 per year. Times were hard even though the costs for goods and services were low.

The depression and economic strife it created did not curb the enthusiasm of visionaries driven to find better ways to communicate. While families were struggling to stay afloat, innovators were developing the foundation of new communication technologies that would change the way the world communicates.

On June 19, 1934, the United States (U.S.) President, Franklin D. Roosevelt, signed the Communications Act of 1934 into law.[1] This act established the Federal Communications Commission (FCC) agency that regulates all interstate and foreign communication by wire and radio, telegraphy, telephone and broadcasts such as Short Message Service (SMS) texting.

During the past decade, all forms of electronic communication have flourished and SMS texting has been a key driver of that growth. There are over 378 Million wireless subscribers in the United States, and smartphone users are sending and receiving over 1.9 Trillion-text message annually.[2] According to the International Smartphone Mobility Report by mobile data tracking firm Infomate, Americans allocate over 30 minutes a day for their texting activities. Now that's a lot of texting!

The FCC Protects Consumer Privacy with TCPA Legislation

Under the direction of the Federal Communications Commission (FCC), the Telephone Consumer Protection Act of 1991 (TCPA) became law.[3] The statute was created to protect consumers from uninvited telemarketing calls, faxes and text messages. On February 15, 2012, the FCC revised its TCPA guidelines; further restricting telemarketing calls.[4] Adjustment of the TCPA requires the prior written consent for most automated telemarketing communications, particularly those made to wireless phones. However, health care communications has its own set of rules.

Healthcare Exemptions to the TCPA

The American Association of Healthcare Administrative Management (AAHAM) lobbied for an exemption from the prior express consent rule for "healthcare-related messages" found in the TCPA for electronic communication subject to the Health Information

Portability and Accountability Act (HIPAA). The FCC issued a Declaratory Ruling and Order[5] on July 10, 2015, addressing several provisions of the TCPA.

The HIPAA exemption in the TCPA rule clarifies the requirements for calls, texts to wireless, and residential landline phone numbers. Under the exemption, communications that deliver a healthcare message made by or on behalf of a "covered entity" or its "business associate" as defined in HIPAA[6] do not require the prior written consent of the party called.

The FCC further clarified that when an individual provided his or her wireless phone number to a healthcare provider, it constitutes permission to contact that number as long as the calls or texts are limited in scope to the purpose of the number provided.[7] Healthcare providers can rely on this provision as constituting prior express consent under the TCPA.

Legislative changes to the TCPA have opened the door for health care providers to adopt texting as an uncomplicated and reliable way to communicate with their patients. Texting now affords healthcare providers a cost efficient avenue to communication internally between staff members and externally between other physicians, hospitals, and patients. This emerging business strategy offers providers new ways to improve patient relations and reduce operating expenses.

TCPA Requirements for Healthcare Text Messaging

Health care providers who deliver exempt "health care messages" must meet stringent requirements to remain in compliance with the TCPA. The following are seven key actions that require adherence:

1. Text messages must be sent to the wireless telephone number provided by the patient;
2. Text messages must state the name and contact information of the health care provider;
3. Text messages are strictly limited to the purposes permitted and must not include any advertising or promotional information; may not include accounting, billing, debt-collection, or other financial content; and must comply with HIPAA privacy rules;
4. Text messages are limited to 160 characters or less in length;
5. A health care provider may initiate only one text message per day, up to a maximum of three messages per week;
6. A health care provider must offer recipients easy means to opt out of future messages; and
7. A health care provider must honor the opt-out requests immediately.

Risks of Text Messaging with PHI

Every form of HIPAA compliant communication encompasses some level of risk. Communication by text with patients and other clinicians provides a divergent set of risks that, like other communication methods, requires adhering to compliant practices to ensure the privacy and security of protected health information (PHI) exchanged. Unlike some electronic communications that do not store interactions between parties, text messages could be stored on wireless devices indefinitely so it poses a risk that unauthorized third parties could access PHI. In addition, even though wireless carriers encrypt text messages there are substantial security threats where sophisticated computer hackers may intercept and decrypt messages.

The HIPAA privacy rule allows individuals the right to access and amend their PHI. If text messages include clinical information, there poses a compliance risk if patients cannot access or amend those text messages.

Providers cannot mitigate risks if they do not identify and carefully document threats to using electronic methods of sending PHI. Examples of threats include:

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

The use of text messaging in healthcare adds to the rapidly increasing threat for data breaches. According to the 2016 Bitglass Healthcare Breach Report there was an 80 percent increase in large-scale data breaches in 2015 and those breaches affected over 10 million people.

The Bitglass Report indicates that:

- One in three Americans was a victim of healthcare data breaches;
- More than 111 million individuals' data was lost due to hacking or IT incidents;
- There were 56 breaches in 2015, up from 31 in 2014;
- Only 97 breaches were due to loss or theft, down from 140 in 2014; and
- Only 5 percent of healthcare organizations use single sign-on security measures for Google Apps or Microsoft Office 365.

The statistics listed in the Bitglass Report encompasses data gathered from the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal. As required by section 13402(e)(4) of the HITECH Act, any breach of unsecured PHI affecting 500 or more individuals must be reported. There are no reporting requirements for PHI breaches affecting under 500 individuals therefore, it is impossible to know how many PHI breaches happen every year. Regardless, it is clear that the full scope of PHI

losses is a growing problem. The rapid rise of new communication technologies will only add to the risks and complications of communicating with a patient.

Security Measures to Protect Text Messages with PHI

If a provider is considering using text messaging as a way to communicate with patients, developing a risk analysis and management strategy to lessen the chance of a breach is of paramount importance. Based on the outcome of a risk analysis, a provider is better able to implement suitable controls to protect the organization.

Examples of security controls include:

- Creating a policy prohibiting the texting of PHI or limiting the type of information shared via text message;
- Carrying out workforce training on the approved use of job-related texting;
- Implementing password protection protocols for mobile devices that create, receive, or maintain text messages with PHI;
- Keep an inventory of all mobile devices used for texting PHI;
- Properly disposing of mobile devices that have been used for the texting of PHI; and
- Ensuring that all texts that include PHI gets notated in their medical record.

To protect providers from the risks of implementing texting in a health care setting, the U.S. Department of Health & Human Services outlined a five-step process that organizations can follow to manage texting with mobile devices.

STEP 1 - DECIDE

Decide whether mobile devices will be used to access, receive, transmit, or store patients' health information or used as part of your organization's internal networks or systems (e.g., your EHR system).

Understand the risks to your organization before you decide to allow the use of mobile devices. Risks (threats and vulnerabilities) can vary based on the mobile device and its use. Some risks may be:

1. A lost mobile device
2. A stolen mobile device
3. Inadvertently downloading viruses or other malware
4. Unintentional disclosure to unauthorized users when sharing mobile devices with friends, family and/or coworkers
5. Using an unsecured Wi-Fi network

You can watch the Mobile Device Privacy and Security video series, which provides scenarios of some of the common risks you may face when using a mobile device for patient care. The videos explore mobile device risks and discuss privacy and security safeguards you can put into place to mitigate the risks.

STEP 2 - ACCESS

Consider how mobile devices affect the risks (threats and vulnerabilities) to the health information your organization holds.

Conduct a risk analysis to identify the risks to your organization. If you are a solo provider, you may conduct this risk analysis yourself. If you work in a larger organization, the organization may conduct the risk analysis.

A risk analysis will help determine the safeguards, policies, and procedures your organization needs. It should include reviewing risks created by all mobile devices used to communicate with your internal networks or systems, regardless whether the devices are personally owned or provided by the organization.

Perform a risk analysis periodically and whenever there is a new mobile device, a lost or stolen device, or suspected compromised health information.

After conducting a risk analysis, document:

1. Which mobile devices are being used to communicate with your organization's internal networks or system (e.g., the EHR system or Health Information Exchange (HIE)),
2. What information is accessed, received, stored, and transmitted by or with the mobile device, and
3. HHS OCR HIPAA Security Series Basics of Risk Analysis and Risk Management

STEP 3 - IDENTIFY

Identify your organization's mobile device risk management strategy, including privacy and security safeguards.

The purpose of a mobile device risk management strategy is to develop and implement mobile device safeguards to reduce risks (threats and vulnerabilities) identified in the risk analysis. The risk management strategy should include evaluation and maintenance of the mobile device safeguards you put in place.

Read more about mobile device privacy and security tips and information you could consider as part of your strategy.

Implementing text messaging as a method for better serving the patient is gaining acceptance from patients and providers. 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 imperative to recognize both the value and risks of texting and to proactively address the issues.

STEP 4 – DEVELOP DOCUMENT and IMPLEMENT

Develop, document, and implement the organization's mobile device policies and procedures to safeguard health information.

Organizations should develop and implement reasonable and appropriate policies and procedures to safeguard health information, including those specific to mobile devices. Here are some topics and questions to consider when developing mobile device policies and procedures:

1. **Mobile Device Management**
    - If the organization allows the use of mobile devices, what should the organization do about managing the use of mobile devices?
        - Has the organization identified all the mobile devices that are being used in the organization? How is the organization keeping track of them?
        - Has the organization assigned responsibility to check all mobile devices used for remote access, to find out if selected security/configuration settings are enabled?
        - Should there be a regular review and audit of the mobile devices?
2. **BYOD (Bring Your Own Device)**
    - Should the organization let providers and professionals use their personally owned mobile devices within the organization?
    - Should providers and professionals be able to connect to the organization's internal network or system with their personally owned mobile devices, either remotely or on site?
3. **Restrictions on Mobile Device Use**
    - Does the organization restrict how providers and professionals can use mobile devices?
        - Can providers and professionals use mobile devices to access internal networks or systems, such as an EHR?
        - Are providers and professionals restricted from using mobile devices when they are away from the organization?
        - Can providers and professionals take their mobile devices home?
        - Should the organization allow texting or emailing of health information?
4. **Security/Configuration Settings for Mobile Devices**
    - Will the organization institute standard configuration and technical controls on all mobile devices used to access internal networks or systems, such as an EHR?
        - If so, is the organization's current mobile device configuration document, including connections to other systems/applications, inside and outside of the firewall.
5. **Information Storage on Mobile Devices**

    - Are there restrictions on the type of information providers and professionals can store on mobile devices?
        - If so, where and for how long should the data be stored?
    - Are providers and professionals allowed to download mobile applications to mobile devices? If so, what type(s) of applications are approved?
6. **Misuse of Mobile Devices**
    - Does the organization have written procedures for addressing misuse of mobile devices?
7. **Recovery/Deactivation of Mobile Devices**
    - Does the organization have procedures to wipe or disable a mobile device that is lost or stolen?
    - Does the organization have standard procedures to recover mobile devices from providers and professionals when their employment or association with the organization ends?
8. **Mobile Device Training**
    - How is the organization training its workforce (management, doctors, nurses, and staff) on policies and procedures?
    - How does the organization hold its workforce (management, doctors, nurses, and staff) accountable for non-compliance?

STEP 5 – TRAIN
Conduct mobile device privacy and security awareness and training for providers and professionals.

Providers and professionals who use mobile devices must have privacy and security awareness and training to avoid costly mistakes that can result in loss of patient trust. Safeguards will not protect health information unless the workforce (including management, providers, professionals, and staff) is aware of its role in following and enforcing those safeguards. Privacy and security awareness and training should be ongoing and include a discussion of the following topics:

- Risks (threats and vulnerabilities) when using mobile devices for work
- How to secure mobile devices
- How to protect and secure health information
- How to avoid mistakes when using mobile devices

Security awareness and training should be easy to use and understand and should support the policies and procedures developed and put in place in response to the risk analysis and risk management strategy.

Finally, the organization should train its workforce so that they understand their mobile device policies and procedures and how to follow them.

Summary

Mobile messaging and texting has become a key industry initiative. Healthcare stakeholders have embraced mobile communication as evidenced by their participation and volume of text conversations. With the advent of the Affordable Care Act, the demand for mobile messaging as a patient engagement tool has steadily increased. It is apparent that mobile messaging, including text, web and chat communication will ultimately be a mainstream healthcare communication method.

Strong communication is essential for care coordination and the use of proper communication tools and channels help providers communicate and provide care across the entire wellness continuum. Texting is only going to evolve, and health organizations must consider the various risks and take the appropriate measures to ensure the safety of PHI.

References:

1. United States Publishing Office, U.S. Code › Title 47 › Chapter 5 › Subchapter I › § 151 https://www.gpo.gov/fdsys/search/search.action?na=&se=&sm=&flr=&ercode=&dateBrowse=&govAuthBrowse=&collection=&historical=false&st=citation%3A47+USC+151&psh=&sbh=&tfh=&originalSearch=&fromState=&sb=re&ps=10&sb=re&ps=10
2. Year-End U.S. Figures from CTIA's Annual Survey Report http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey
3. Federal Communications Commission Washington, D.C. 20554 In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, https://apps.fcc.gov/edocs_public/attachmatch/FCC-12-21A1.pdf.
4. FCC Adopts Rules to Strengthen Consumer Protections Against Unwanted Telemarketing "Robocalls" to Wireline and Wireless Phones, https://www.fcc.gov/document/fcc-strengthens-consumer-protections-against-telemarketing-robocalls-0.
5. Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991; American Association of Healthcare Administrative Management, Petition for Expedited Declaratory Ruling and Exemption; et al, https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order
6. Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/
7. Free-To-End User Financial and Healthcare Alerts: The FCC Applies Common Sense, With Limitations (FCC TCPA Order Report Parts 7 & 8 of 11) By Blaine C. Kimrey, Lisa M. Simonetti & Bryan K. Clark, http://www.mediaandprivacyriskreport.com/2015/09/free-to-end-user-financial-and-healthcare-alerts-the-fcc-applies-common-sense-with-limitations-fcc-tcpa-order-report-part-7-of-11/
8. Cell Phone Activities 2012, http://www.pewinternet.org/2012/11/25/cell-phone-activities-2012/