The CIO's Guide to HIPAA Compliant Text Messaging

Executive Summary

The risks associated with sending Electronic Protected Health Information (ePHI) via unencrypted text messaging are significant, especially given the climate of rising enforcement of compliance with The Health Insurance Portability and Accountability Act (HIPAA) and The Health Information Technology for Economic and Clinical Health (HITECH) Act. However, there is high demand amongst healthcare providers to use text messaging as a fast, convenient way to communicate and collaborate with colleagues.

This whitepaper provides:

- A detailed overview of the HIPAA Omnibus Rule, including HITECH Meaningful Use mandates, as it pertains to secure texting messaging of ePHI
- Best practices for instituting a secure text messaging policy within your healthcare organization
- A vendor comparison checklist for meeting HIPAA, security, administrative, security and vendor requirements

About ecfirst (Home of The HIPAA Academy)

ecfirst, home of the HIPAA Academy, delivers deep expertise to healthcare covered entities, business associates and health IT vendors with its full suite of services that include:

- Risk Analysis and Technical Vulnerability Assessment
- Contingency Planning/Business Impact Analysis (BIA)
- Policy Templates (available for HIPAA Privacy, HIPAA Security, ISO 27000, PCI DSS)
- On-Demand Compliance & Cyber Security Remediation Services
- Managed Compliance Services Program (MCSP) for continual HIPAA and HITECH compliance
- Certified HIPAA Professional (CHP) & Certified Security Compliance Specialist (CSCS) Training Programs
- HIPAA Evaluation Seal for Business Associates

About Imprivata

Imprivata is the leading global provider of healthcare IT security solutions. Imprivata Cortext enables clinicians to securely send text and picture messages from their smartphone, tablet or computer, which improves efficiency, enhances patient care and helps healthcare organizations address the deficiencies of pagers and other outdated communication technologies. Imprivata Cortext, a secure text messaging application for healthcare, has been Validated as HIPAA Compliant by ecfirst.

The Risk of Insecure Texting

The risks associated with sending Electronic Protected Health Information (ePHI) via unencrypted text messaging are significant, especially given the climate of rising enforcement of compliance with The Health Insurance Portability and Accountability Act (HIPAA) and The Health Information Technology for Economic and Clinical Health (HITECH) Act. However, there is high demand amongst healthcare providers to use text messaging as a fast, convenient way to communicate and collaborate with colleagues.

This whitepaper discusses the key steps an organization can take to enable clinicians to use text messaging while ensuring that HIPAA and HITECH compliance requirements are met. These steps include:

Step 1 - Policy: Establish an organizational policy
Step 2 - Product: Identify an appropriate text messaging solution
Step 3 - Practice: Implement and actively managing the text messaging solution

HIPAA and HITECH Compliance Mandate

The HIPAA Security Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf) requires organizations to address text messages as part of their comprehensive risk analysis and management strategy. Based on the risk analysis, the organization must determine the appropriate administrative, physical and technical controls to mitigate the risks of sending ePHI via text messaging.

In order to determine the technical security measures necessary to comply with this standard, covered entities must review the current methods used to transmit ePHI. The covered entity must then identify the available and appropriate means to protect ePHI as it is transmitted, select appropriate solutions, and document its decisions. The Security Rule allows for ePHI to be sent over an open, electronic network as long as it is adequately protected.

Another area of compliance impacted by texting is the HITECH requirements for breach notification. The HIPAA Final Rule states that "breach" is defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of such information. Devices used for texting, such as smartphones and tablets, may be lost or stolen, so the importance of ensuring HITECH compliance in the event of a breach is an area that must be reviewed in the context of text messages that may reside on the compromised device.

Step 1 - Policy: Text Messaging

The scope of an effective policy pertaining to the use of text messaging must apply to the organization in its entirety, including all employees, physicians and affiliates. In addition, some third parties, including contractors and vendors, may be required to abide by parts of the policy if required by the organization through a Business Associate Agreement (BAA). Further, the policy must apply to the network, systems and applications that process, store or transmit ePHI or other sensitive information.

A policy for secure text messaging should include the following key statements, which establish the minimal requirements for the organization:

- Text messages are electronic communications sent with a mobile device or computer system. Text messages can transmit photos, videos and written word formats of communication. If the content of such a message contains ePHI, then the text message must comply with HIPAA requirements.
- All text messages containing ePHI must be sent in a secure, encrypted and approved format.

The following requirements must be met when ePHI is transmitted, stored or processed via a text messaging application:

Policy Statement		Current Policy Status
Users should not send text messages containing ePHI unless the text message is encrypted both in transit and at rest using an appropriate application. Additionally:	The text message must be communicated from the sending device, through the mobile provider or a software application to the recipient's device in an encrypted manner	
	The encrypted text message should not be decrypted and stored on the cellular provider's systems in ways that can be accessed by unauthorized personnel	
If an employee wishes to send ePHI via text message to another employee, both the sender(s) and the receiver(s) must fulfil both the encryption requirements for the message in transit and at rest.		
All users who wish to send or receive text messages containing ePHI must ensure that the IT-approved secure text application is approved by the IT department for such purpose. Specific requirements include:	The employee must submit their mobile device number with the help desk or the IT department to ensure that proper inventory is maintained of all mobile devices sending or receiving ePHI	
	Mobile devices used to text ePHI must be properly sanitized upon retirement of the device. The IT department must securely wipe	

Policy Statement		Current Policy Status
	all mobile devices when they are returned. If an employee is using a personal device, they must contact the IT department to securely wipe the device prior to returning it to their cellular provider	
An effective policy for the use of secure text messaging should mandate that the following safeguards be implemented by employees sending and/or receiving messages:	The mobile device or secure texting application must be password protected; this feature must never be disabled	
	The mobile device must be configured to lock automatically after a period of inactivity (not to exceed 5 minutes)	
	All text messages containing ePHI should be limited to the minimum information necessary for the permitted purpose. Multiple identifying factors (e.g., full name, date of birth, medical record number, social security number or condition specific information) should not be used	
The following seven guidelines must be followed when texting PHI. Ensure the accuracy of the information being texted by administering the following precautions:	Confirm the recipient of your text	
	Confirm delivery and receipt of the text. A confirmation receipt that the information was received is ideal	
	Do not use shorthand or abbreviations	
	Review texts prior to sending to ensure accuracy. Beware of autocorrect functions	
	Do not text patient orders	
	ALL text messages (or annotations of text messages) that are used for clinical-decision making are documented in the medical record	
	Delete all texts containing ePHI as soon as the information is no longer readily needed	
Other policy statements to consider and adopt based on your organization's compliance mandates, include:	Report all unencrypted text messages that are received or sent out that contain any ePHI immediately to the HIPAA Security Officer or the IT Department	

Policy Statement		Current Policy Status
	Report all text messages that are sent to the wrong intended individual to the HIPAA Security Officer or the IT Department	
	Every policy and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later	
	Log-in audit information and logs relevant to security incidents must be retained for six years	

Step 2 - Product: Checklist for a Secure Texting Solution

To ensure compliance with HIPAA requirements and enable clinicians to use text messaging securely, organizations should work with vendors that meet all of these key capabilities

HIPAA Security Compliance Requirements

Key Capability	Description	Vendor A	Vendor B
Authentication methods	Provides secure authentication methods to ensure authorized access		
	End-to-end authentication environment		
Password management	Passwords generated/used are of sufficient complexity		
	Secure password change/reset mechanisms		
Administrator rights	Administrative rights must be separate from regular user rights		
Login monitoring	All login attempts, both successful and failures, are logged and monitored		
	Accounts are locked after a defined number of failed login attempts		
Automatic logoff	Users are logged out of the application after a period of inactivity		
Access control	Controls are in place to ensure users can only access messages they sent or received		
	All administrative access and actions are logged including administrative password resets for users		
Unique user identification	Users are uniquely identified throughout the application and all actions can be tied directly to these ID's		
Access control audits	Ability to generate reports on access controls, including administrative actions		
Account authorization and establishment	Only administrative users have the ability to create new accounts		
	Account creations and modifications are logged		
Account	Accounts can be terminated by an		

Key Capability	Description	Vendor A	Vendor B
termination	administrator		
	Terminated accounts are prohibited from accessing any previous messages and are unable to send new messages		
Audit capabilities	Logs all user actions related to authentication and message access		
	Logs all administrative access related to managing users and elevated access activities		
	Logs are time stamped for easier correlation		
Transmission security	Ensures data is protected while in transit		
	Transmission security provided independent of the transmitting platform		
Protection of data on the mobile device	Messages stored on a mobile devices are encrypted independently of any native device encryption		
	Any proprietary data cached on the device, such as staff directory information, is also encrypted		
	Encryption algorithms used are industry standard AES256		
	Resetting the application password destroys all saved messages		
Backup processes	All messages are archived to allow administrative access		
	Message archives are encrypted and stored securely. Third party storage does not have access to archived ePHI.		
	Message retention time is customizable to match the organizational policy		
	Access to message archives is restricted		

Usability, Administrative & Security Requirements

Key Capability	Description	Vendor A	Vendor B
Usability Requirements			
Cloud-hosted solution	Solution is a cloud-hosted SaaS and does not require on-premise infrastructure or hardware.		
Secure photo sharing	Allows photos to be taken and attached to text messages		
	Photos cannot be shared or accessed outside texting application		
Designed for texting across multiple organizations	Users can text across multiple organizations from within a single application		
	Users with multiple organization accounts can have a unified inbox and contact directory		
Notifications & read receipts	Notifications & read receipts provide visual indicator and time stamp of when recipient has or has not read message		
Callback requests	Call back requests that enable recipient to call back with a single tap, embedding phone number directly into message		
Streamlined contact directory	Enables users to search, find and text all contacts in application directory without ever typing a phone number		
	Administrator can populate contact directory via webform, csv. import or AD synchronization		
Customizable sounds	Enables users to set tone of sound alert when receiving a new message		
Administrative & Security Requirements			
Microsoft Active Directory synchronization	Add/remove/modify users directly through current Active Directory (AD) infrastructure		

Key Capability	Description	Vendor A	Vendor B
	Administrator can setup AD sync, without sending users to vendor, etc.		
Secure Notifications	Messages notifications displayed contain do not include any ePHI		
Remote wipe for lost or stolen devices	Administrators can disable accounts which revokes access to all messages and information		
Prevention of EPHI leakage from the messaging environment	Incorrectly entering the PIN on the mobile device a certain number of times destroys any saved data		
	Copying messages from the application to the clipboard is disabled		
Maintain organizational privacy	Restricts 3rd parties from having access to PHI		
Set message life span	Enables administrator to set how long messages will persist within application on device		
Optional App PIN	Administrator can set additional PIN on application		
Vendor Requirements			
Trusted Business Associate	Vendor provides Business Associate Agreement for secure texting solution		
Certified by independent 3rd party	Vendor solution has been audited and certified by 3rd party. Vendor has training and procedures in place to properly handle PHI		
Financial viability	Additional security products to support a more complete ecosystem and financial stability		
Industry Experience	Several (at least 5+) years of experience in healthcare security		

Step 3 - Practice: Tracking & Monitoring

Once a secure text messaging solution is deployed, it is critical to ensure active management to maintain compliance with HIPAA and HITECH requirements. This includes monitoring log files and other audit information to ensure appropriate use. Specifically, IT administrators should:

1. Track and monitor administrator activities related to managing users and policies
2. Ensure that authentication events are appropriately captured
3. Ensure that message read receipts are time stamped.

Importantly, organizations should ensure that a proactive audit practice aligns with an established policy is implemented for managing the secure and HIPAA-compliant text messaging framework.

The Bottom Line for HIPAA Compliant Texting

The risks associated with exchanging ePHI via unsecured text messages are significant, especially in light of specific compliance mandates such as HIPAA and HITECH. By following the guidelines and steps outlined in this paper, organizations can properly identify a secure text messaging solution that satisfies the clinical need for faster, more efficient communication while also meeting IT security and compliance requirements.

References

HIPAA 164.310(a)(1)
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

American Reinvestment and Recovery Act of 2009 (ARRA)/(HITECH)
http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf

Corporate Office
295 NE Venture Drive
Waukee, IA 50263 USA
Toll Free: 1.877.899.9974 x17
Phone: 515.987.4044 x17
Fax: 515.978.2323
www.ecfirst.com

Worldwide Headquarters
10 Maguire Road, Building 1
Lexington, MA 02421-3120 USA
Phone: 781 674 2700
Toll-free: 1 877 663 7446
Fax: 781 674 2760
http://www.imprivata.com/cortext