DrFirst®

HIPAA Compliance and Secure Messaging

Corporate Headquarters
9420 Key West Ave., Ste. 101
Rockville, MD 20850
Toll Free (866) 263-6511

West Coast Office
1640 South Stapley Dr., Ste. 122
Mesa, AZ 85204
(602) 466-7547

sales@drfirst.com | www.drfirst.com | blog.drfirst.com

Ref ID: DF02012018-1

HIPAA Compliance and Secure Messaging

Table of Contents

DrFirst®

Practical | Powerful | Innovation

Physicians, nurses, and other members of the care team bring their smartphones to work, like workers in any industry. Healthcare providers want that same convenience of text messaging for their everyday clinical communications, many of which contain protected health information (PHI).

Texting has many benefits for communication. It allows for immediate notification and response, but without time and intrusion of a phone call. Additionally, since nearly everyone has a smartphone with them throughout the day, it's readily available. This level of communication has many benefits in the healthcare environment.

There are many ways that texting can help improve and streamline communications in healthcare. For example, pharmacists can clarify prescriptions with the prescribing physician, or nurses can confirm discharge instructions with physicians quickly and efficiently. Physicians can also consult with others across the care spectrum. In fact, 50% of hospital-related medication errors and 20% of ADEs are attributed to poor communication at transition of care.[1]

However, HIPAA compliance can be compromised if healthcare providers send PHI over unsecure messaging systems. This concern over HIPAA compliance keeps many organizations from endorsing text messaging for care providers, or even forces them to put policy restrictions around it.

While the HIPAA security rules may not explicitly mention text messaging, they do require covered entities to protect access to PHI in electronic systems. This includes the servers used to deliver text messages and the devices that send and receive PHI.

From a compliance perspective, covered entities must ensure that any PHI sent and received by its providers is adequately protected. Unfortunately, standard text messaging systems do not have the necessary protections to comply with HIPAA protections for PHI. There is no auditing around the storage and access of PHI sent via text messages, different systems have varying standards for data retention in their services, and PHI on a non-protected application is subject to unauthorized access.

How is your organization addressing text messaging?

Certainly, some care providers already use text messaging in their jobs, while many others want to be able to text each other for consultations or questions. With text messaging already a risk factor in the clinical environment, organizations need a strategy for addressing it. Like many new threats, responses vary from ignoring the problem to employing defensive strategies that are difficult to enforce and unlikely to succeed in the long run.

Setting up policies and procedures that ban text messaging from within the facility or campus may seem prudent, however, once employees are off the premises, it's out of your control. This strategy positions the IT team as enforcers rather than enablers, potentially harming other technology initiatives. This is the proverbial "carrot or the stick" scenario, and when it comes to change management, the carrot tends to be more successful.

Hospitals and healthcare providers nationwide might have **avoided nearly 2,000 patient deaths — and $1.7 billion in malpractice costs** — if medical staff and patients communicated better.[2]

Relying on policies and training to prevent PHI compromise is another approach to ensure HIPAA compliance. This involves training providers on what constitutes PHI and counting on them to be careful not to include it in text messages. However, to be successful, this approach requires ongoing effort, and offers little guarantee that no PHI is being compromised.

Other organizations ask care providers to carry separate devices, provisioned and maintained by the IT team and running secure applications. Purchasing and provisioning smart phones is a costly option for organizations with large and dynamic work forces. Care providers must either carry both their own personal devices and the provisioned device, or use the work device for personal applications.

Given the options above, it is clear healthcare organizations need a better strategy for handling text messaging that supports care providers in their daily work while meeting HIPAA standards for information privacy and protection.

To be truly effective, a texting tool must be specifically designed for use in healthcare environments; it must be designed to help providers achieve better care coordination, better health outcomes, better transitions of care and lower hospital readmissions. It must also meet all of HIPAA's security standards, guarding patients, caregivers and medical facilities against unintended disclosure of protected health information.

To ensure adoption by healthcare staff, the texting tool must include functionality that both streamlines clinical communications, and improves healthcare workflows include, such as:

- Administer users, rights and privileges
- Private, group or patient-specific care team chats
- Create and monitor user groups
- Search and control message content
- Track user analytics and insights
- Message and audit trail search, retention and archiving
- Event notification distribution to internal and external providers
- Supports clinical content sharing in virtually any format

Ten ways to address HIPAA compliance using secure messaging

1. Policy

Make sure to implement a policy based on the HIPAA guidelines that documents the user's responsibilities when using secure messaging on mobile devices and personal computers.

Creating or updating your organization's policies and procedures in these areas is a critical step to ensuring HIPAA compliance. One of the first areas to address given the change in technology, is the Bring Your Own Device (BYOD) policy. In the past, many healthcare organizations would not allow employees to use their own devices for any work-related functionality.

With the availability of secure messaging platforms, however, these policies are beginning to change. App-based tools provide a secure environment regardless of whether it is on a personal or work device, so organizations can rest assured that they will remain in compliance with HIPAA while allowing their care team the convenience of using their own devices.

By bringing your policies in line with the ever-changing work environment, institutions can improve compliance and decrease resistance to the necessary workflows. The less you can disrupt an end user's daily workflow, the more likely it is they will comply with the rules.

The less you can disrupt an end user's daily workflow, the more likely it is they will comply with the rules.

2. Separating healthcare-related texting

Although it may not map directly to any HIPAA compliance initiative, treating healthcare-related texting differently than personal texting is essential and helps reinforce compliant behavior.

Standard text messages are easily available to anyone who picks up the device receiving the text. The organization also has no insight into, or control over, where and how data is stored and protected by the telecom carrier.

3. Authentication and authorization for access to text messages

Once healthcare texting is separated, the next step in meeting HIPAA requirements, specifically the Security Rule, is to put authentication and authorization controls around messaging.

With a secure solution, the organization controls access and authorization and the privileges associated with healthcare-related messaging. The hospital administrator must explicitly invite the care provider to join. The provider then downloads the app to his or her smartphone. Organizations can further protect access to the application on the device by requiring users to enter a PIN to access their messages.

In this way, users can have confidence that the person to whom they are sending PHI is in fact the care provider associated with that hospital.

4. Encryption of data in the network and in transit

Standard SMS text messages are not inherently secure in transit. While the carrier may encrypt messages over the network, the messages themselves stored in the service are unencrypted, and the carrier can access that data without that access being audited.

A secure solution will use the cellular data network or a Wi-Fi network for exchanging information and encrypt all transmissions using TLS/SSL to ensure all PHI is secured. In addition, transmissions between all server nodes in the service are encrypted, so data is also always encrypted while in transit.

5. Encryption of data on the mobile device

The content of a traditional text message is available to anyone who picks up the device. If the message includes PHI, this puts HIPAA compliance at risk. Most secure solutions do not download any data to a mobile device unless attachments are explicitly downloaded and saved (with the appropriate warnings).

6. Removal of PHI from screen notifications

Using native texting tools, you often see the content of a text when it arrives on your phone. For a text that contains PHI, this could create a HIPAA violation, as PHI is potentially exposed to anyone near the phone when the text arrives.

A secure messaging solution keeps PHI out of notifications altogether. The notification pop-up only shows the fact that the message arrived, with the sender's name and organization name.

Specifically, HIPAA audit controls require "hardware, software and/or procedural mechanisms that record and examine activity..." related to ePHI.[2]

7. Messaging archiving

Using unsecured text messaging, users are subject to mobile carriers that have different policies around retention of text data. Some may retain the data for a few days, though not necessarily on a secure server. Others do not archive the text messages at all, but retain information about when and where texts were sent, also known as metadata.

This archiving is not guaranteed to be HIPAA-compliant.

8. Integrated auditing

Of course, audits are a crucial component to HIPAA compliance. Specifically, HIPAA audit controls require "hardware, software and/or procedural mechanisms that record and examine activity..." related to ePHI.[1]

This level of auditing is not possible with traditional text messaging.

9. Secure sharing of attachments

The ability to attach a photo, video, pdf, audio clip to a request for information can accelerate communications. However, attachments must also be considered private, particularly when associated with PHI.

When using traditional text messaging, there is no way to ensure these attachments are secure. However, by employing a secure messaging solution, an organization can ensure they have control over how these attachments are sent and downloaded.

A secure messaging solution often uses multiple mechanisms to protect PHI residing within the app on a mobile device.

10. Instant lockout for lost or stolen devices

The downside of the convenient mobile form factor is that smartphones are easily lost or stolen. And if that smartphone has access to PHI, this mobility increases the potential HIPAA risk.

A secure messaging solution often uses multiple mechanisms to protect PHI residing within the app on a mobile device.

The application can be protected with a personalized PIN, preventing access from someone other than the owner who picks up the phone. It often also has a 'time-out' period after which it prompts for the PIN, which can be configured to meet the organization's needs.

Where to go from here?

Now that we have laid out 10 reasons that secure messaging can improve communication, workflows, and patient safety while ensuring HIPAA compliance, the next step is finding the right solution.

Here at DrFirst, we offer a secure messaging platform called Backline®. As part of our larger suite of full lifecycle medication management solutions, we allow providers, pharmacists and clinical staff to handle every obstacle along the continuum of care.

To learn more about Backline visit www.drfirst.com/platforms/secure-messaging

1. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

2. https://www.statnews.com/2016/02/01/communication-failures-malpractice-study/

DrFirst, the nation's leading provider of ePrescribing and medication management solutions, enables stakeholders across the healthcare industry to intelligently utilize comprehensive real-time data and connectivity to increase their patient safety ratings, efficiency and profitability. Today, over 170,000 healthcare professionals and over 60% of Electronic Health Record vendors, depend on DrFirst's innovative software solutions to improve clinical workflows, expedite secure collaboration across a patient's care team and drive better health outcomes. The company's integrated technologies include its award-winning electronic prescribing platform, the most comprehensive medication history available, clinically specialized secure messaging, as well as patient medication adherence monitoring and benefits checking. In addition, DrFirst was the first to offer e-prescribing for controlled substances (EPCS), and is considered the industry standard for providers nationwide. For more information, please visit www.drfirst.com or connect with us @DrFirst.

DrFirst®

Sales	**(866) 263-6511**
Customer Support	**(866) 263-6512**
	www.drfirst.com

DrFirst®

Corporate Headquarters
9420 Key West Avenue,
Suite 101
Rockville, MD 20850

Satellite Office
12800 Middlebrook Road
Suite 400
Germantown, MD 20874

West Coast Office
1640 South Stapley Drive
Suite 122
Mesa, AZ 85204

Sales	**(866) 263-6511**
Customer Support	**(866) 263-6512**
Main Number	**(301) 231-9510**
General Inquiries	**(888) 271-9898**

www.DrFirst.com | sales@DrFirst.com