imprivata®

Ten Ways Imprivata Cortext Adds HIPAA Compliance to Text Messaging

cortext™

Healthcare is not immune to the 'consumerization of IT' that's happening in other industries. Physicians, laboratory technicians, nurses and other care providers bring their own smart phones to work, just like everyone else. Accustomed to convenient text messaging in their personal lives, many want to use the same text messaging for work-related, clinical communications that may contain protected health information (PHI).

Texting has many benefits as a communications medium: it's immediate but doesn't demand the real-time interruption of a phone call. With everyone carrying a cell phone, it's readily available. Text messaging has many benefits in the healthcare environment. For example, pharmacists can clarify prescriptions with the prescribing physician, or nurses can confirm discharge instructions with physicians quickly and efficiently through text messaging. And of course physicians can consult with others quickly and easily. Texting has the potential to streamline clinical communications in healthcare.

But HIPAA compliance can be compromised if healthcare providers send PHI over unsecure text messaging infrastructures. Serious concerns over HIPAA compliance keep many organizations from endorsing or supporting text messaging for care providers, or force them to put policy restrictions around it.

While the HIPAA security rules do not explicitly mention text messaging, they do require covered entities to protect access to PHI in electronic systems. This would include the servers used to deliver text messages and the devices (personal or otherwise) that send and receive PHI. From a compliance perspective, covered entities (hospitals) must ensure that any PHI sent and received by its providers is adequately protected. Unfortunately, consumer-focused text messaging does 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 ISPs have different standards for data retention in their services, and PHI in the clear on mobile phones is not protected from unauthorized access.

WHAT'S YOUR TEXTING STRATEGY?

It's safe to assume that some care providers already use text messaging in their jobs. And many others want to be able to text each other for consultations or questions. With text messaging already a factor in the clinical environment, organizations need a strategy for addressing it.

Some organizations employ defensive strategies that are difficult to enforce and unlikely to succeed in the long run.

- Policies banning texting of healthcare related information altogether. You can set up policies and procedures that ban text messaging from within the organization facility or campus. Once people are off the premises, however, it's out of your control. This strategy positions the IT team as enforcers rather than enablers, potentially harming other technology initiatives.
- Relying on policies and training to prevent PHI compromise. Another strategy is to train providers on what constitutes PHI and count on them to be careful not to include it in text messages. This strategy requires ongoing effort on everybody's part, and it's difficult to ensure that no PHI is being compromised.
- Provisioning secure devices and messaging applications. Some 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.

Clearly healthcare organizations need a different strategy for handling text messaging that supports care providers in their daily work while meeting HIPAA standards for information privacy and protection.

IMPRIVATA CORTEXT HIPAA COMPLIANT TEXT MESSAGING

Imprivata works with many hospitals and healthcare organizations to offer fast, secure access to electronic medical records using Imprivata OneSign®. Seeing the growing need for secure, HIPAA compliant text messaging, Imprivata worked closely with care providers and healthcare IT administrators to define and create a solution that meets specific clinical needs. The objectives are simple:

- Reduce risk of HIPAA violations
- Streamline communications and workflows for healthcare providers
- Support fast, affordable implementation in diverse healthcare environments

The result of this work is Imprivata Cortext – a free, HIPAA compliant text messaging service that lets care providers text patient information without putting patient privacy at risk. It meets the security requirements of HIPAA, but shields the users from impact of the extra security. In fact, Cortext adds features that streamline clinical communications, so care providers benefit from transparent security as well as improved workflow. These features include:

- Access to the organization contact directory to find colleagues quickly
- Call back requests that enable the recipient to call back with a single tap
- Group messaging across multiple organizations for improving care team communications
- Notifications and read receipts for message senders, so they can determine if the recipient has read the message or not

Cortext is available as a native iPhone and Android application, so care providers can use their personal devices. A web-based chat console supports providers when at a workstation. This allows a nurse, for example, to use Cortext for Web on any workstation.

The solution itself is hosted in the cloud, so organizations do not need to provision server hardware to deploy it. The mobile apps use cell phone data networks or Wi-Fi connectivity, not the text messaging networks run by the mobile carriers.

At its core, Imprivata Cortext is designed to enable HIPAA compliant text messaging, which requires protecting the entire, end-to-end environment with authentication and encryption technologies. The following section describes the overall security and compliance measures built into Cortext.

TEN WAYS IMPRIVATA CORTEXT ADDS HIPAA COMPLIANCE TO TEXT MESSAGING

Imprivata Cortext protects and audits access to PHI that may be contained in text messages, whether the data is in transit, in servers and storage, or on mobile devices. Cortext uses a layered approach to ensuring HIPAA compliance throughout the service, as described below. Because of these attributes, any "covered entity" using Cortext can demonstrate that they are safeguarding ePHI in text messages.

1. Segregation of Healthcare-Related Texting

Although it doesn't map directly to any HIPAA compliance initiative, treating healthcare-related texting differently than personal texting is essential.

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

Cortext separates HIPAA compliant text messaging from native text messaging, so organizations can control where and how data is stored and accessed. Care providers no longer need to worry about identifying and removing PHI from text messages related to patient care.

2. Authentication and Authorization For Access to Text Messages

Once healthcare texting is segregated, the next step in meeting HIPAA requirements (specifically the Security Rule) is to put authentication and authorization controls around Cortext.

With Cortext, IT staff controls access/authorization and the privileges associated with healthcare-related texting. The hospital administrator must explicitly invite the care provider to join Cortext; the provider then downloads the app to their smart phone. Cortext automatically generates a unique user name and password for the device, not visible to the end user. Organizations can then protect access to the application on the device by requiring Cortext users to enter a PIN to access their messages.

In this way, Cortext users can have confidence that the person to whom they are sending the PHI is in fact the care provider associated with that hospital, and not someone claiming to be that person or not truly affiliated with the hospital.

3. Encryption of Data in the Network and in Transit.

Ordinary 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.

Cortext uses the cellular data network or a Wi-Fi network for exchanging information and encrypts all transmissions using TLS/SSL to ensure all PHI is secured. In addition, Imprivata Cortext uses encrypted transmissions between all server nodes in the service, so data is always encrypted while in transit. And all data is encrypted on disk using AES-256 encryption.

4. 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.

Cortext encrypts data at rest on the smart phone:

- If a provider works with multiple organizations, conversations for each organization are stored separately and protected with AES-256 encryption.
- Any proprietary data cached on the device, such as staff directory information, is also encrypted with AES-256 encryption.
- The AES key is optionally protected with the user's PIN. (You need the PIN to access the encrypted data.) Destroying the key disables access to those conversations.

5. Removal of PHI from Screen Notifications

Using native texting tools, you 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.

Cortext keeps PHI out of notifications. The notification pop-up only shows the fact that the text arrived, with the sender's name and organization name.

6. Messaging Archiving

Using native (unsecured) text messaging, mobile carriers have different policies around retention of text data. Some retain the data for a few days, 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.

Imprivata has built an archiving layer into Cortext that complies with HIPAA security requirements. The archive itself is encrypted, access controlled and backed up. The length of data retention depends on the needs of the organization. For free, Cortext provides a 30-day rolling archive retention. Organizations can also choose to extend their archive retention with Cortext Premium. Visit www.cortext.com/what's-free.

All messages that originate and terminate in the same organization are archived and encrypted with a public key assigned to the organization. Messages crossing organization boundaries are not archived.

7. Integrated Auditing

How often does the word 'audit' come up in a discussion on HIPAA compliance? HIPAA audit controls require "hardware, software and/or procedural mechanisms that record and examine activity…" related to ePHI.

Cortext automatically audits and logs:

- All administrator activities related to managing users
- Activities related to managing policies
- All authentication events
- Read receipts (time stamped)

8. Secure Photo Sharing

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

Imprivata Cortext lets healthcare providers take and attach pictures from within the Cortext application along with text messages. Photos received or taken through Cortext do not go into the device's photo album but remain in Cortext, so they cannot be shared outside of Cortext. All picture texts are audited as part of the service.

9. Prevention of PHI Leakage from the Messaging Environment

All the work done to protect access to PHI within the secure texting environment is undermined if someone can easily cut and paste protected information from a text message into an email, document, social media site or other application on the device. Cortext disables copying message data to the clipboard.

Cortext provides reports such as the Administrator Activity Report, with the ability to filter data in support of audit activities.

10. Instant Lockout for Lost or Stolen Devices

The downside of the convenient mobile form factor is that smart phones are easily lost, left in cabs, or stolen. And if that smart phone has access to PHI, this mobility increases the potential HIPAA risk.

Imprivata Cortext uses multiple mechanisms to protect private health information residing within the Cortext app on a mobile device.

- The Cortext application can be protected with a personalized PIN, preventing access from someone who picks up the phone. It also has a configurable 'time-out' period after which it prompts for the PIN.
- The application can automatically lock out a user after a number of unsuccessful authentication attempts
- The organization administrator can disable the account through the Cortext Admin Console (and set up the user with a new device when appropriate).
- Data on the phone itself is encrypted. Disabling the account destroys the encryption key for that device, automatically making the encrypted data on that device essentially inert.

IMPLEMENTATION DETAILS

Healthcare IT departments are busy rolling out technology to support Meaningful Use, leaving no extra bandwidth for deploying and managing heavyweight messaging applications. This is why Imprivata chose to offer Cortext as a cloud-based service supported by widely available iOS and Android devices.

The communication infrastructure for Cortext is hosted on Imprivata servers in the cloud, so organizations do not need to install or configure servers. It requires no hardware purchases. A web-based administrative console enables easy administration out of the box.

In addition, Imprivata offers an Active Directory Connector, delivered as a virtual appliance, that keeps Cortext synchronized with a hospital's Microsoft Active Directory. This means that the Cortext directory is always up-to-date with the latest personnel and updates are automatically distributed to end users through Cortext.

Cortext is a free service for any healthcare organization. Additional services such as extended message archiving are available with Cortext Premium which includes the following:

- Access to the Cortext Directory Connector to provide automated updating of contact details
- 90-day rolling cloud archive retention
- Enterprise support: phone, email and forum support with a 4 hour SLA.

The basic process of implementing Cortext is as simple as the following:

1. Enroll for free at www.cortext.com
2. Add your users via the web admin center by webform entry, .csv import or synchronization with your Active Directory
3. Invite your users with an email or printed invitation

ABOUT IMPRIVATA

With more than 2 million users and 900 healthcare customers, Imprivata is the #1 provider of secure access solutions for healthcare. By strengthening user authentication, streamlining application access and simplifying compliance reporting across multiple computing environments, customers realize improved workflows, increased security and compliance with government regulations.

APPENDIX: HIPAA SECURITY RULE REQUIREMENTS AND CORTEXT

Cortext meets all of the standards laid out for the electronic communication of PHI including authentication, authorization, encryption, archiving and auditing. The table below summarizes the Standards and Implementation Specifications that Imprivata Cortext addresses.

Standard **Standard number** *Implementation Specification*	***Cortext Capability***
Access Controls **163.312(a)(1)** *Unique user identification* 1643.312(a)(2)(i) *Automatic Logoff* 164.312(a)(2)(iii)	*Cortext uses unique username and password to authenticate with the messaging server. Cortext for iPhone and Cortext for Android can be set up to require a four-digit PIN to access by the administrator.* *An inactivity setting automatically times out sessions on Android, iPhone or Web and Admin Console*
Encryption 164.312(a)(2)(iv)	***Cortext messages**: All data is encrypted within Cortext's storage and in communications between nodes.* ***Cortext for iPhone and Android:** Conversations and proprietary data for each hospital is encrypted on every mobile device using AES-256, protected with the user's PIN. Destroying the PIN removes access to the data.* ***Cortext for Web:** No permanent data is stored in web browser, and non-caching directives are used.*
Transmission Security 164.312(e)(1)	*All data in transit is secured with TLS AES-256 and RSA 2048. No PHI is exchanged with web services, and all credentials and invitation codes are also encrypted using TLS.*
Person or Entity Authentication 164.312(d)	*A user is first provisioned with an invitation code from an administrator, which expires in seven days. Credentials generated during sign-up are stored on the mobile device for subsequent authentication when the user provides a four-digit PIN.* *Credentials on device are protected using AES-256 encryption.*
Audit Controls 164.312(b)	*Cortext automatically logs the following:* - *All administrator activities related to managing users and policies* - *All authentication events* - *Time-stamped message delivery and read receipts*
Workforce Security 164.308(a)(3) *Termination procedure*	*Administrators can disable users using the Admin Center or by disabling the user AD. Once disabled, users cannot access the directory or any messages belonging to that hospital stored on the mobile device.*
Security Awareness and Training 164.308(a)(5) *Login Monitoring* *Password Management*	*Cortext restricts access to the application until the correct PIN is entered.* *Web users can change their passwords or request a password reset using an invitation code issued by the administrator.*

Worldwide Headquarters
10 Maguire Road, Building 4
Lexington, MA 02421-3120 USA
Phone: 781 674 2700
Toll-free: 1 877 ONESIGN
Fax: 781 674 2760

www.imprivata.com