athenaText℠ Security Frequently Asked Questions

Enabling HIPAA Compliance

Q: How does athenaText enable HIPAA and HITECH compliance?

A: athenaText provides several features to enable your HIPAA and HITECH compliance. These include:

- Message encryption
- Unique user identification
- User authentication
- App autolock after a period of inactivity (duration may be adjusted in settings)
- Data integrity controls

While athenaText provides the features you need to comply with HIPAA and HITECH, organizations are ultimately responsible for their HIPAA compliance policies.

Q: Who can send and receive messages within athenaText?

A: Any athenaNet user can communicate via athenaText within the web, inside athenaNet or via the mobile application. Additionally, users can invite other health care professionals to join athenaText to build their network, and choose to use only the mobile application. The mobile application is available, for free in the App Store or Google Play, for any health care professional, regardless if you are an athenaNet user.

- **Web (athenaNet) users:** Any athenaNet user with the athenaText permission (included in the athenaClinicals permissions) can send and receive messages within athenaText. These athenaNet users will automatically be connected to anyone else in their practice that has the athenaText permission enabled. In addition to communicating via athenaText with other users in their practice, these users are able to improve communications across practice silos by inviting other health care professionals, outside their organization, to connect with them via athenaText.
- **Mobile users:** Mobile-only users can access athenaText by downloading in the App Store or Google Play as a standalone, and / or by accepting an invitation from an existing user. If the recipient of the invite has an NPI number and they go through the verification process, they can also invite others to join athenaText. If they do not have an NPI number, they can only text with the person who sent the invite. The intent is to ensure those who can send and receive athenaText messages are verified health care professionals.

Q: Why can only NPI holders, not tied to an athenahealth organization invite others to join athenaText?

A: athenaText was designed specifically for health care professionals to efficiently and securely collaborate care. To limit usage to health care professionals, users must go through the verification process and enter their NPI number.

Q: How does athenaText protect data integrity?

A: Ensuring integrity of PHI is standard within the HIPAA Security Rule. athenaText protects data integrity in several ways:

- Application sandboxing on mobile devices helps assure messages are not altered or destroyed by other apps running on the device while the messages are being processed or stored.

- Communication between devices and athenaNet uses internet-standard TLS, which provides as part of its design data integrity protection to ensure data is not altered or corrupted in transit.
- athenaNet messaging services operate within secure, highly-protected athenahealth data centers with limited access to a very small number of systems administration personnel.

Mobile Message Storage

Q: Does athenaText store messages on my mobile phone?

A: Yes, the data is encrypted and stored in the application's database on both iOS and Andriod devices. Messages are stored on your device until you delete them.

Q: How does athenaText encrypt messages stored on my mobile phone?

A: Messages (text and images) are stored on your device in encrypted format using SQLCipher. On Apple devices, AES256 encryption is used. On Android, the encryption is AES128.

Q: Are pictures taken with other apps encrypted?

A: Taking pictures directly in the athenaText application is the recommended method for pictures associated with PHI. Pictures taken directly in the application are encrypted and unlike pictures taken from your built-in photo gallery on your device, the pictures are not stored locally on your device. athenaText will not encrypt pictures on your device's built-in photo gallery, so if you take a picture using the built-in camera application on your mobile phone, then send that picture via athenaText, that picture will remain unencrypted within your device's photo gallery, but will be encrypted within athenaText.

Q: Are communications being transmitted encrypted on my mobile phone?

A: Messages (text and images) sent and received within athenaText are encrypted while they are being transmitted to and from your device. This encryption uses industry-standard TLS encryption meeting HITECH requirements. Currently supported TLS ciphers are TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, and TLS_RSA_WITH_3DES_EDE_CBC_SHA. Athenahealth may change the supported cipher suites, for example to add support for newer ciphers.

Q: How can I protect access to the athenaText app on my mobile phone?

A: Any athenaNet user will be required to enter a PIN specific to athenaText unless they have chosen to use implementation MDM security (such as AirWatch). In this case, you must assert you have an automatic device lock feature enabled that requires a passcode or a fingerprint to unlock. The athenaText specific PIN is separate from any PIN used to unlock your device. If you use an athenaText PIN, you are prompted for the PIN when the app enters the foreground, at a frequency determined by your athenaText app settings: immediately, after one minute of inactivity, or after five minutes of inactivity.

Q: What happens if I enter an incorrect PIN too many times?

A: To help guard against someone trying to guess your athenaText PIN, when an incorrect PIN is entered four consecutive times, the athenaText app wipes all athenaText data (including messages stored on the

device) and returns itself to a reset state. In this state, the user would not need to repeat the verification process, but would be required to enter their username and password.

athenaNet Message Storage

Q: Does athenaText store messages in athenaNet?

A: Messages sent and received with athenaText are stored in athenaNet, athenahealth's cloud-based platform for providing technology services and solutions for the health care industry. athenaNet's messaging services are the delivery agent for messages. A device sends a message to athenaNet, and athenaNet stores the message for delivery. The message is delivered real-time if the recipient is connected to a network, or the message is delivered when the device reconnects to a network.

Q: How long are messages stored on the server-side, in athenaNet, if the recipient is not connected to a network?

A: The server will hold the messages until the recipiant's device connects to a network and the athenaText app checks for messages.

Q: How long are messages stored in athenaNet?

A: Messages are retained within athenaNet for a minimum of seven years. Messages stored in athenaNet are not deleted when they are deleted from your device. Messages stored in athenaNet are not accessible without special assistance from athenahealth personal.

Q: Are messages stored in athenaNet encrypted?

A: Messages stored in athenaNet using data-at-rest AES256 encryption. Athenahealth has access to the messages.

Mobile Usage

Q: How does athenaText affect my HIPAA risk analysis?

A: From a security risk perspective, mobile devices are similar to laptops. They are portable, can contain sensitive information, may be lost or stolen, can be picked up and used by family members or friends, have their screens visible in public places, may be in the possession of employees who are terminated, can be connected to untrusted networks, and can be subject to computer viruses and other malware. For the purpose of HIPAA risk analysis, it is important to consider what new risks are created within your organization by the use of mobile devices with PHI, and how those risks will be managed and mitigated.

Q: What is the verification process for mobile only users not tied to an existing athenahealth organization?

A: A Lexis Nexis and AMA/NPPES verification process has been created to ensure that any health care professional not tied to an organization in athenaNet and only using the mobile application, is a verified health care professional. If the mobile user opts out of the verification process, they can only text with the people that have invited them to join their athenaText network. If you are a member of a health care organization that purchased athenaClinicals or athenaCoordinator, your organization verifies your identity

and your need to access PHI, and also provides your athenaText account in athenaNet and on the mobile application so verification is not necessary for athenaNet users.

Q: Should I consider mobile security awareness training?

A: Security awareness and training can be one of the most effective ways to prevent security breaches. You may want to consider what kinds of security awareness and training your health care organization should receive associated with the use of mobile devices with PHI. Training topics covered could include:

- Your mobile device policies and procedures
- Risks with mobile devices
- How to safeguard access to your mobile devices and the athenaText application (e.g. unique PIN)
- Proper use of mobile devices in coordinating care

Q: What guidelines should I consider for mobile usage at my organization?

A: Organizations may benefit from guidelines for using mobile devices in the provision of health care and the sending / receiving of PHI. These guidelines may include basic information such as:

- Safeguarding PIN codes or other credentials used to access the device
- Not "jailbreaking" the device
- Making sure an unlocked device can't be picked up and used by someone else
- Making sure PHI is messaged only with athenaText

The guidelines should also consider to what extent critical information can be conveyed in messages and whether any messaged information could affect patient safety or be considered part of someone's medical record.