e-Net Messenger Security Features & FAQs

1. *Does e-Net Messenger meet HIPAA requirements?*

Yes - it meets HIPAA Security and Privacy standards.

- Business Associate Agreements are accepted

2. *What is the software scheme?*

e- Net Messenger utilizes a Client/Server scheme with client applications that run on:

- Windows based PC's (Windows XP & later)
- iOS mobile devices v4.3 & later
- Android mobile devices v2.2 & later
- Blackberry is not compatible

3. *What is the server scheme & security/reliability?*

The server is a web hosted solution - no local server is required, so users don't need to worry about hosting.

- Server Redundancy and Security Features:
  - Automatic Generator Backup
  - Multiple Internet connections
  - 24/7 video surveillance
  - 24/7 guarded hosting facilities

4. *How is e-Net Messenger data secured?*

- All messages, including subject, message body and attachments are encrypted before transmission
- Stored messages including attachments on client devices are fully encrypted using AES encryption
- Stored messages including attachments on GD-Net server are fully encrypted using AES encryption
- User credentials on server side are fully encrypted using AES encryption
- User credentials and administrative configuration on client devices are encrypted using AES encryption
- Transmission of messages to/from clients/server are fully encrypted
  - PC based e-Net Messenger uses AES encryption communicating with the GD-Net server via HTTPS
  - Mobile (iOS/Android) e-Net Messenger uses AES encryption communicating with the GD-Net server via HTTP
  - All messages transmitted are not only sent over an encrypted channel, but the messages themselves are also encrypted
- User account is locked if client device tries to log in with wrong password multiple times

5. How are e-Net Messenger attachments (pictures, videos, etc) protected from improper use?

- A user cannot send/receive messages to/from destinations outside of their e-Net Messenger organization
  - Organization administrator controls which devices can see which other devices (users)
- Messages and attachments are stored encrypted, and cannot be opened via file browsers
- Organizational administrator can set auto-delete time for old messages
- For iOS devices, all messages and attachments are contained within the e-Net Messenger app, and are NOT available from Photo Album or other apps
  - This capability cannot be guaranteed for pictures taken on Android devices in the current release v2.1.0.3
- Android devices and PC's open attachments in 3rd party applications (such as Windows Media Player for playing videos, Adobe Reader for viewing PDF's, etc)

6. Who can e-Net Messenger message with?

e-Net Messenger only communicates with permitted destinations (contacts) that are pre-configured by the organization administrator. The admin can define the destination linkages and which destinations appear in the list. For example; Ambulance can message with the CAREpoint at the hospital, but cannot see the Physicians' mobile devices – but the CAREpoint can see both Ambulances and Physicians.

- e-Net Messenger can message with single individuals, multiple individuals or groups
- Destinations are not stored locally on client device (pulled from server during sign in process)

7. Are there Admin configurable settings & features?

Additional (optional) security features of e-Net Messenger include:

- Require password every time app is launched
- Automatically lock app after configurable idle period and require password to unlock it
- Automatic time stamped audit trail logging and uploading
- Automatically delete sent and/or received messages after user configurable time period
- Configurable to only allow pictures/videos taken from within e-Net Messenger (don't allow importing from device photo album/gallery)
- Organization administrator can set their own AES encryption key for all of their devices
- Client device user settings are password protected and password can be changed by organization administrator

For more information, contact General Devices' Tech Support:

201.313.7075 (voice)
201.313.5671 (fax)
support@general-devices.com (e-mail)
or visit our web site at www.general-devices.com