CAREpoint™ Workstation

e-Bridge™ Mobile Telemedicine

e-Bridge The future of connected care

Overview

Enhanced patient care by providing your on-scene view directly to physicians, specialists and hospitals anywhere, anytime. With e-Bridge you can document and share voice, text, photos, data, video clips & live streaming easily using your mobile device or PC in a HIPPA secure environment/application. Enhance decision support, documentation of trauma, stroke, burns, refusal of treatment, sending 12-leads, mobile forms, location & real-time ETA tracking, Mobile Integrated Healthcare / Community Paramedicine and much more.

e-Bridge Feature & Benefits

- Pre-Arrival Notification
- Refusal Documentation
- Decision Support
- Disaster Response Coordination
- Triage / Field Hospital secure communications
- Medical Team Preparation
- Scene Documentation
- Simplify EMS Reporting
- Consolidate EMS & Hospital Communications
- CAREpoint Integration (Pre-Hospital Communication workstation)
- FDA Listed, HIPAA certified, Strong encryption
- Fully featured for today's healthcare needs
- Short learning curve with easy operation

e-Bridge™ Mobile Telemedicine

Statement of differentiation

- If the intended use of a device or software involves the treatment or diagnosis of patients, and not just post incident documentation, the device and/or software is considered a medical device by FDA federal law.
    - GD is an FDA registered manufacturer in good standing and GD's e-Bridge Mobile Telemedicine application and CAREpoint Workstation are listed/cleared devices with the FDA.
    - As an FDA registered company, GD is compliant with the **21 Code of Federal Regulation (C.F.R.) Part 820 Quality System Regulation for medical devices**. This requires GD to comply with **FDA mandated Design Control methodologies** in its development to ensure the efficiency and safety in our products, keeping patient/end user's safety as top priority in all our solutions. This also means GD gets periodical inspections by the FDA to ensure that we are compliant throughout the life cycle of our products from idea to **post market surveillance** activities.
    - Other recent messaging applications currently on the market (Twiage, Pulsara) are not FDA registered and can only transmit pictures of single or 12-lead printouts – for non-diagnostic purposes, and are unable to connect to the medical devices in a legal regulated capacity. These companies are required to have disclaimers on their websites. Unapproved use puts the using organization at legal risk.
- GD is an established company with an exceptional track record of nearly 30 years in the EMS-Hospital communications market. GD solutions handle over 10,000 call daily. GD is backed by in-house R&D, manufacturing and 24/7 technical support.
- GD's HIPAA and security are backed by 3rd part audit

Additional Information: e-Bridge The future of connected care

e-Bridge Security Features & FAQs

1. ***Is e-Bridge HIPAA compliant?***

   Yes – e-Bridge complies with HIPAA Security and Privacy standards for business associates.
   - Business Associate Agreements are accepted
   - GD's HIPAA and security are 3rd party certified

2. ***What is the software scheme?***

   e-Bridge 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

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-Bridge 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-Bridge uses AES encryption communicating with the GD-Net server via HTTPS
     - Mobile (iOS/Android) e-Bridge 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-Bridge attachments (pictures, videos, etc.) protected from improper use?***
    - A user cannot send/receive messages to/from destinations outside of their e-Bridge 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
    - Pictures/videos taken within the e-Bridge app DO NOT appear in the devices default Photo Album or gallery
    - For iOS devices, all messages and attachments are contained within the e-Bridge app
    - For Android devices and PC's, all messages are contained in the e-Bridge app and some attachments require a 3rd party applications (such as Windows Media Player for playing videos, Adobe Reader for viewing PDF's, etc.)

6. ***Who can e-Bridge message with?***

    e-Bridge 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-Bridge 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-Bridge 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
    - E-Configurable to only allow pictures/videos taken from within e-Bridge (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

And The Survey Says . . .

- Survey of EMS providers and medical directors about the operational uses for telemedicine conducted by the National Public Safety Telecommunications Council (NPSTC) found strong support…
    - 64% thought live video or images could assist with real-time critical care support
    - 61% thought video or images could result in better decision-making and risk mitigation on patient refusal requests
    - 57% thought telemedicine could help with decision making and support for mobile integrated healthcare and community paramedicine visits
    - 67% thought video could give hospital ED greater awareness of the status of incoming patients
    - 60% believe video could aid in stroke, STEMI or trauma team activation
    - 61% believe it can result in improved patient care due to better visualization of the scene or mechanism of injury
    - 60%+ believe video/pictures can be useful in post-incident training or quality assurance