STARTEL® Secure Messaging

ADVANTAGES OF THE STARTEL SECURE MESSAGING APPLICATION

- **Persistent Alerts**
- **Device Receipt Notifications**
- **Read Receipt Notifications**
- **Separate boxes for Encrypted & Unencrypted Messages**
- **Detailed Documentation & Reporting**
- **Full Audit Trails**
- **Immediate Peer-to-Peer Message Delivery**
- **Secure / Encrypted Messaging**
- **Ability to Send to Groups or Individuals**
- **Specific Application Password Protection**

What is Startel Secure Messaging?

Startel Secure Messaging is an application that allows you to send messages between devices in a manner that is not readable by anyone but the intended recipient, thus assuring not only compliance with Privacy Rules & Regulations, but also the peace of mind that comes from knowing confidential information will remain confidential.

Startel's Secure Messaging is *Peer-to-Peer*

Peer-to-Peer refers to a type of direct communication between devices that does not require an intermediate server or website. The advantage of *Peer-to-Peer* messaging is its lack of dependence on a centralized system, which can be a potential point of failure. In a model utilizing a central server, if the server is down, all incoming and outgoing communications are down. In the *Peer-to-Peer* model, messages are sent directly from one device to another, with no need for a web site or server. Peer-to-Peer messaging is more open, dependable, flexible, capable, and convenient.

Secure Peer-to-Peer Messaging is Peer-to-Peer communication that adds the ability to encrypt and decrypt the messages that are sent and received. Thus, with Startel's Secure Messaging Application, as long as the device that you're sending to has the application (and has been issued a Registration ID), you will be assured of *secure* communication, with no need to log into a central website to send or retrieve messages.

Why is the Ability to Send Secure Messages Important?

Multiple pieces of legislation enacted by Congress—including the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH), the 1999 Graham-Leach-Bliley Act (GLBA), and the 2002 Corporate and Auditing Accountability and Responsibility ACT (aka Sarbanes-Oxley, or SOX)—contain requirements for ensuring the safety of private information. Furthermore, new privacy provisions associated with the HITECH Act now apply to not only "covered entities," but also business associates of covered entities. Business associates now "bear the responsibility and liability for any breach in incidents involving unsecured protected health information."

Transmitting "Protected Health Information" (PHI) via Startel Secure Messaging ensures not only the desirable result of keeping private information private, but also compliance with all of the above acts.

Startel Secure Messaging Implements Secure Socket Layer (SSL) Technology

Startel's Secure Messaging Application utilizes SSL technology—the same technology that protects sensitive information on major websites that offer secure online transactions. An SSL Certificate enables encryption of sensitive information during transmission—the SSL Certificate being a unique credential generated by a Certificate Authority (CA), which authenticates the identity of the Certificate Owner. Thus, Startel's Secure Messaging offers compliance, privacy, and Sender/Receiver authentication. Startel's Secure Messaging SSL technology is *256-bit encrypted*—exceeding the standards necessary for legal compliance.

STARTEL

If you can dream it, STARTEL *can build it!*

STARTEL *innovation….often imitated, but never equaled!*

16 Goodyear
Irvine, California 92618
(800 - 782-7835) DIRECT

SALES
Sales@startel.com

MANAGEMENT
Comments@startel.com

SUPPORT
Techsupport@startel.com

Startel Secure Messaging: HIPAA, HITECH, GLBA and SOX Compliant

Startel has developed a Secure Messaging Application that ensures full compliance with HIPAA, HITECH, GLBA, and SOX. The Startel Secure Messaging application ensures that PHI is…

- ✓ Stored securely
- ✓ Encrypted when transmitted
- ✓ Protected upon delivery
- ✓ Fully HIPAA, HITECH, GLBA and SOX Compliant

Startel Sales Model

If you are a customer of Startel's SMS Aggregator Service, you will be provided access to the Startel Secure Peer-to-Peer Messaging Application FREE of charge, and will have complete control of its distribution to clients. You can choose to charge a fee, or not. At Startel, our goal is to increase your profitability and efficiency by creating useful applications that you can sell to *your* clients.

Is Startel Secure Messaging Available on Multiple Platforms?

Yes, the Startel Secure Messaging Application is available for a variety of mobile operating systems / platforms, including: iOS® (for iPhone®, iPad®, iTouch®), Android® OS, and Blackberry® OS.

What if I Lose My Phone?

The Startel Secure Messaging Application provides the ability to password protect the application itself. With this additional layer of security added to the password protecting your smart phone, sensitive data stored on your smart phone's Secure Messaging Application need never be compromised, even if you lose your phone.

Two Steps for Getting Started

There are two simple steps for getting started using Startel's Secure Messaging Application:

Step 1: Download the Application as directed by the Product sponsor. The Startel Secure Messaging Application can be downloaded to a variety of mobile platforms/operating systems—including Apple iOS® (iPAD®, iTouch®, iPhone®); RIM Blackberry® OS (all Blackberry Models); and Android® OS (any smart phone utilizing the Android mobile operating system).

Step 2: Enter a Unique Registration ID. Once you've received a unique Registration ID from your hospital administrator or call center sponsor, and have entered it into your application, you're ready to begin sending and receiving secure messages. It's that simple!

Are Secure Messages Stored on the Phone Itself?

Yes, the secure messages that you receive on your smart phone remain on your phone until you choose to delete them. This is particularly helpful if you need to access a particular message, but you are not in a WIFI or Internet enabled area.

Is There a Record of my Secure Messages?

Yes, the Startel Secure Messaging Application provides a full audit trail of your Secure Messages, including information like:

- ✓ Device Notification date/time stamps
- ✓ Message Downloaded date/time stamps
- ✓ Message Read date/time stamps (optional)
- ✓ Message Reply date/time stamps (optional)
- ✓ Message "Filed" date/time stamps (optional)

Is Reporting Available?

Yes, there is a full line of Activity and Billing reports available for the Startel Secure Messaging Product.