



Secure Health Messaging

Clinician notification has emerged as an essential part of healthcare delivery and workflow. The ability to notify and provide physicians, nurses and other clinicians with critical patient information in a timely manner improves the quality of patient care, response time and the cost of healthcare.

Secure Health Messaging is the most effective and enhanced method of delivery of Protected Health Information (PHI) to clinicians' mobile phones via HIPAA compliant SecureSMS text messaging technology.

Whether it be critical lab results, on-call physician notification, physician order or request for patient information, critical notification must obtain the following two essential components: notification and secure delivery of patient data.

Notification

Cell phones were not designed to handle complex data, transactions, graphics and lengthy text messages. Standard SMS is typically assumed delivered as soon as the carrier submits the message over their network without having any confirmed response from the recipient's mobile handset. Hence, there is no definitive way to determine if a message was received by the recipient or whether it was opened or just simply deleted. Standard SMS does not provide timing around any of these events and the sender has no information regarding the delivery of the message as soon as the content leaves the portal or the sender's cell phone.

Notification by definition requires that the sender is aware of the end result. Meaning that the sender must be aware of the time which a message is delivered to the recipient's cell phone, and the exact time when the message is opened and viewed.

At the same token, the sender should be alarmed when a message cannot be delivered or has not been viewed past a predetermined amount of time.

In healthcare environment where a timely delivery of vital information can result in saving lives, critical physician notification must pass strict standards and uncompromising delivery mechanism that takes the guesswork out of patient workflow. Nothing should be left to chance.



With Secure Health Messaging Micro Client technology, all of outgoing messages receive confirmation of delivery and read with the exact date and time stamp. For incoming messages, Micro Client automatically issues a temper-proof acknowledgment to the sender via SecureSMS Gateway when the message is received or read by the recipient. In addition to audit logs, a Delivery Log Dashboard Application allows senders to view the status of all sent messages. The web-based dashboard application displays information in real-time such as recipient names, sent, delivery and read times and a built-in alarm system that notifies senders if a message is not viewed within a predetermined time frame.

Secure Delivery of Patient Data

Standard SMS (text messaging) is neither secure nor in compliance with HIPAA regulations and standards of encryption. The delivery of Protected Health Information (PHI) to cell phones and PDAs should only be facilitated by utilizing Advanced Encryption Standard

(AES). The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) [PDF, 273K] on November 26, 2001 and is adopted as an encryption standard by the U.S. government.

The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plain text. AES is one of the most popular algorithms used in symmetric key cryptography.

A number of elements need to function harmoniously for a message to be sent securely from a portal or a cell phone to another cell phone.

Micro Client

Secure Health Messaging Micro Client is a light application that installs on the handset to communicate with Secure Health Messaging Gateway. The application is similar to a regular SMS editor and encrypts outgoing secure messages as well as decrypts incoming secure messages received via Secure Health Messaging Gateway.

Secure Health Messaging Micro Client is password protected and erases secure messages upon unauthorized access attempts. When issued by Secure Health Messaging Gateway, the remote wipe feature removes all secure messages on the handset in the event the phone is lost or stolen.

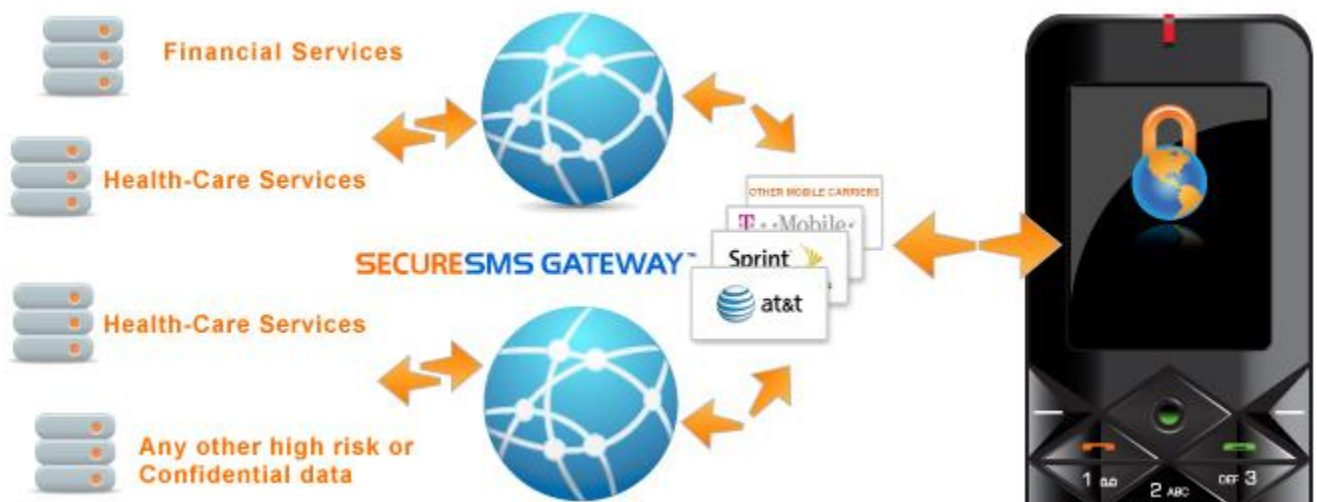
All of the outgoing messages receive confirmation of delivery and read with the exact date and time stamp. For incoming messages, Micro Client automatically issues a tamper-proof acknowledgment to the sender via Secure Health Messaging Gateway when the message is received or read by the recipient. An intelligent self-updating feature ensures the mobile phone is always operating with the latest version of Secure Health Messaging and is benefiting from its most recent features.

Gateway

The CellTrust Secure Health Messaging Gateway is a pioneering, first of its kind, secure bridge to facilitate communication between applications and carriers around the world via the SMS channel. Secure Health Messaging Gateway offers message encryption, routing, storage, reporting, compliancy and other advanced features required to manage SecureSMS Micro Client remotely such as data wipe, configuration settings and updates.

CellTrust combines established industry security best practices and patent-pending Secure Health Messaging™ technology to lay a secure foundation for mobile communication via the SMS channel. While keeping security at the forefront of design and development, CellTrust sets itself apart from SMS providers who achieve security - but as an afterthought. From physical security to proper system lockdown and hardening of the servers; multiple layers of security protect communication, hardware and software from unauthorized access at CellTrust.

Access to Secure Health Messaging Gateway is similar to using a standard SMS gateway. Both secure messages and standard SMS messages are submitted from application using a set of high-level APIs. Messages received from organizations are identified on the handset by short code number, keyword or any name that is specified by the mobile phone user in the secure phone book. Secure Health Messaging Gateway offers worldwide coverage independent of carrier's SMS coverage area.



Secure Health Messaging Gateway hosted and managed by CellTrust is accessed by network and application over a secure Internet connection such as HTTPS. Performance is scaled via load-balanced server farms, and business continuity is increased by redundant access points to carriers. For additional security, performance and rebranding, a separate instance of the application can be hosted.

On-Site Enterprise Server

Secure Health Messaging Gateway hosted and managed by healthcare organization's IT team sends and receives messages over dedicated short code hosted with any supported aggregator or carrier. Secure Health Messaging is also configurable as Circle of Trust with option to specify own encryption scheme and message archiving for reporting and

compliance. The healthcare organization may request Secure Health Messaging Gateway built to order, or as an appliance deployed at hospital's internal data center.

Healthcare Portal

Healthcare Portal enables clinicians and medical service providers to manage and organize message content. The power of Healthcare Portal is in its configurability and ability to send messages to pre-determined recipients (known as an MT message) then receive and manage the information the recipients send back (known as an MO message). Built to fit the needs of healthcare providers, the Portal allows for strong integration to existing applications, security, customization, collaboration, automation, reporting, remote access and document repository. By utilizing Healthcare Portal, large or small content can be quickly delivered to recipients with auto-trail capability, reply forwarding, auto-trail and detailed reporting.

Add Scheduled Message

Monday, June 8, 2009 3:57:59 PM

Message Content

Title:

Shortcode*:

Keyword*:

Message:

Total number of characters: 215

Timing

When: Day: Month: Year:

What Time: Hour: Minute:

Frequency:

Until: End Date: Month: Year: Number of Times: Never Stop!

Distribution

Send to: Group: Phone (include country code) or e-mail:

Via:

Apply premium charge Apply double opt-in

Templates play an important role in the Healthcare Portal Gateway and application. Highly flexible, templates can be used for several purposes: for frequently used forms, pulling and processing data fields (in the form of tags) for integration to third party systems, and also for message personalization - whereby each physician can see only his or her template in the message.

The screenshot shows a web form titled "Edit Message Template". It is divided into two main sections: "Primary Information" and "Template Body*".

Primary Information

- Title*:** A text input field containing "ResponseToA".
- Type*:** A dropdown menu with "[Please Select]" as the current selection.
- Subject*:** An empty text input field.

Template Body*

Please compose your message template module in the below box. You can use any of predefined tags in the left column or add new tags by putting them in the \${}. For example if you write 'Phone Number', it will be fixed text in the template module, but if you write \${PhoneNumber} it will be considered a 'tag' and will be replaced with a phone number such as '1800888888'. Once you have written your text, click on Process to review the text and tags. In addition to tags, you can also use tokens which are defined in Branding configuration. Tokens are of the form - @@XYZ@@ and they work in a similar fashion as tags.

The template body text area contains the text: "Congrats. U win!".

At the bottom of the form is a "Process" button.