Glob@lCerts

Market Overview:

HITECH and HIPAA:
Briefing for Healthcare IT Security Personnel

HITECH/HIPAA: Privacy Security and Electronic Transaction Standards

Introduction: The HIPAA (Healthcare Insurance Portability Accountability Act of 1996) requirements are a broad based set of mandates covering everything from manual handling of forms to Internet security requirements. Subtitle D of the HITECH (Health Information Technology and Economic Clinical Health) Act passed in 2009 further strengthened the provisions and enforcement. There is no single product or solution that covers all the requirements, but the less user training and overhead a solution requires, the easier the compliance will be to manage and maintain.

The GlobalCerts™ Solution provides user transparent secure delivery of email and attachments to meet HIPAA PHI (Protected Healthcare Information) encryption requirements. Our secure email solution offers your organization the ability to implement a low-cost, easy-to-maintain, standards-based solution.

Protection: "…the secure messaging system must employ high-end encryption, insuring that documents are never exposed, either in transmission or while stored on a server..."

Protection: *"…the secure messaging system must employ high-end encryption, insuring that documents are never exposed, either in transmission or while stored on a server..."*

The SecureMail Gateway™ (SMG) protects your documents with high-end encryption. It supports S/MIMEv3.1 encryption, which leverages the following standard, industry-accepted cryptography algorithms:

- Asynchronous: RSA, DSA, DH
- Symmetric: AES256, AES192, AES128, and 3DES
- Hashing: SHA256

The SecureMail Gateway™ performs encryption on outbound email messages and attachments, and decryption on inbound email messages and attachments, utilizing both public and private keys. These cryptographic keys conform to the X.509v3.0 digital certificate cryptography standard.

Recipients are able to use either S/MIME certificate-based authentication or Web-based secure password authentication, for those recipients that cannot place a digital certificate on their desktop.

Please note that all encryption keys and SecureMessenger™ messages (messages sent to non-S/MIME recipients) are stored securely on the SecureMail Gateway™ appliance in a AES encrypted format at all times. All encryption and decryption operations are transparent to the user.

Identification: *"…an acceptable method that adheres to federal regulations (either in place or pending) of assuring that both the sender and the recipient are known to each other..."*

Identification: "…an acceptable method that adheres to federal regulations (either in place or pending) of assuring that both the sender and the recipient are known to each other..."

The SecureMail Gateway™ provides HIPAA-compliant authentication of sender and recipient. Sender authentication utilizes existing network and mail system credentials and authentication methods; the SMG uses an implicit trust model to encrypt outgoing email messages and decrypt incoming email messages on behalf of your internal users. Recipient authentication utilizes one of the following mechanisms:

- External registered recipients (X.509 certificate holders) authenticate themselves to their existing (locally stored) X.509 certificate;
- External unregistered users (do not possess X.509 certificates) authenticate themselves to the secure message stored encrypted on your SMG and retrieved via an HTTPS secured Web connection
- Passphrases can be set up by the recipient, or by your administrator or sender and communicated to recipients through an out-of-band method (SMS, fax, telephone).

Importantly, SecureMessenger™ permits the sender of an email message to choose a passphrase for authenticating an anonymous (unregistered) recipient for purposes of message retrieval. This passphrase selection process occurs when your sender chooses the message's time-to-live and return receipt settings, as well as the option to save the anonymous recipient's settings for future communications.

Message Authentication: “…verification that the sent message, along with any attachments, is the identical message that was received (message and attachment encapsulation)…”

Message Authentication: *“…verification that the sent message, along with any attachments, is the identical message that was received (message and attachment encapsulation)…”*

The SecureMail Gateway™ supports strong message integrity through the use of digital signatures. A digital signature is made on every outgoing, encrypted email message (both to registered and anonymous users). These signatures utilize the sender’s private key to create a cryptographic hash of the message contents that can be verified only with the corresponding public key of the sender. This signature validation process is performed automatically with all standard S/MIME client applications and through the SecureMessenger™ message delivery mechanism.

User-Friendly: “…the system must integrate with our current email system and provide true user transparency – ideally it should identify and automatically encrypt sensitive messages...”

User-Friendly: *“…the system must integrate with our current email system and provide true user transparency – ideally it should identify and automatically encrypt sensitive messages...”*

The SecureMail Gateway™ appliance integrates seamlessly with an organization’s existing email system, whether it’s Microsoft Exchange, Novell GroupWise, or a hosted solution like Microsoft Office 365.

The SecureMail Gateway™ supports seamless message identification, flagging, and automatic encryption of sensitive messages (including those messages including PHI data) through its Data Leak Prevention (DLP) integration. More information about our content filtering is available from GlobalCerts™.

The SecureMail Gateway™ provides an easy to use, “point-and-type” message designation method on an individual message basis, which allows users to encrypt messages that may or may not have specific PHI information, but are still deemed to contain confidential PHI data. Your organization may determine what keywords it desires to use as this secure message designator. No desktop software install is required for this feature, and system administrators do not need to maintain any client-desktop applications.

Business Solution Scalability: “…the solution must integrate with our existing business practices and have the ability to support future network and user expansions...”

Business Solution Scalability: *“…the solution must integrate with our existing business practices and have the ability to support future network and user expansions...”*

The SecureMail Gateway™ is compatible with all standards-based content filtering, archiving, anti-virus, anti-spam, and email monitoring and management services. The SMG can be integrated easily with an existing external SMTP message relay agent. Any external SMTP message relay agent currently managed by your system administrators can be utilized, unless GlobalCerts™ is contracted directly to perform device management, monitoring, and oversight.

On average it takes approximately 90 minutes for the SecureMail Gateway™ to be remotely installed, configured, and implemented. Administrator training services are included as part of the basic implementation package. Installation times may be significantly decreased with accurate and complete pre-installation information from your system administrators.

Universal Access: "…the system must allow our business partners—as well as our patients—an easy communication method, without the need for special software by any recipient. Recipients must be able to respond to messages in the same secure manner…"

Universal Access: *"…the system must allow our business partners—as well as our patients—an easy communication method, without the need for special software by any recipient. Recipients must be able to respond to messages in the same secure manner…"*

The SecureMail Gateway™ supports email encryption to any recipient on the Internet, even if they do not possess an X.509 certificate, through its SecureMessenger™ feature. It enables these recipients to respond to messages in the same secure manner, including attachments.

SecureMessenger™ utilizes a seamless email-to-Web interface for sending and receiving secure messages to external users that do not have a secure email system or digital certificate in place on their end of the communication.

The SecureMail Gateway™ also works with X.509 certificates that did not originate inside the organization's enterprise network. All message communications between your organization and external users utilize standards-compliant S/MIMEv3.1 cryptography whenever possible. All external registered users with a standards-compliant X.509 certificate are able to communicate seamlessly with your internal users.
The ability to register email recipients that have existing X.509 certificates is fully supported by the SecureMail Gateway™.

The SecureMail Gateway™ is easy to manage and maintain. It requires minimal user or certificate administration. The SMG does not force administrators to perform certificate management activities. There is no certificate lifecycle management overhead, no complex certificate issuance processes, no manual certificate exchange processes, and no heavyweight user registration procedures.

Web Ready: "…users must be able to read their email on their Web device or Internet cell phone and respond without the need to purchase or exchange certificates or keys..."

Web Ready: *"…users must be able to read their email on their Web device or Internet cell phone and respond without the need to purchase or exchange certificates or keys..."*

The SecureMail Gateway™ allows users to read their secure email on their workstation, laptop, tablet or smartphone. They are able to respond just as easily as if they were at their own workstation.

Future HIPAA Support: *"…we need to be able to accommodate changes that may be needed to comply with regulations governing HIPAA…."*

GlobalCerts™ closely monitors all regulatory changes considered or enacted by the U.S. Department of Health & Human Services. The SecureMail Gateway™ is able to accommodate any changes that may be needed for ongoing compliance with the HITECH Act and HIPAA, and their security regulations, including those currently proposed and finalized, and those planned in the future.

Support: "…our organization expects excellent customer and technical support…"

Support: *"…our organization expects excellent customer and technical support…"*

Our customers' success is our most important mission. Technical support from a security expert is immediately available either through email at support@globalcerts.net or by toll-free at (855) 614-CERT. Upon notification, a GlobalCerts™ engineer will assess the cause and severity of the technical support issue, and determine the appropriate course of action.

Take the First Step Towards Seamless Secure Email

The SecureMail Gateway™ makes it simple to send secure messages to anyone anywhere. Tens of thousands of users secure their email on a daily basis with the field-proven GlobalCerts™ solution. Contact us to learn why the SecureMail Gateway™ is fast becoming the healthcare industry's standard for secure messaging, and let us help your organization meet regulatory compliance.

Simply
Securing the Future

117 South 14th Street
Richmond, Virginia 23219
855-614-2378 (Toll Free)

sales@globalcerts.net
www.globalcerts.net