SECTIGO

Securing Emails with S/MIME Certificates for HIPAA Compliance

Email is a must, but email is a vulnerability

As in any industry, email is a critical communication medium for healthcare professionals. Left on its own, however, email is fundamentally insecure for transmitting Personal Health Information (PHI). Email containing PHI must be protected with digital certificates for institutions to successfully guard patients' privacy and maintain compliance with the HIPAA and HITECH regulations.

In particular, all health-related email traveling beyond the firewall requires end-to-end encryption, meaning that email is encrypted in the sending mail server, in all receiving mail servers, and in transit. This encryption prevents any party except the sender and receiver from viewing the content of the email, including the operator of the mail server or any malicious software that circumvents the established email controls. This approach works even with mail servers running in third-party cloud services.

Furthermore, encrypting email is a cost-effective method of meeting HIPAA's email retention requirements without compromising security. Since email content is encrypted prior to archiving, it is protected from disclosure regardless of the manner it is stored. And mail header information is still searchable within the mail application even for encrypted email, making it practical to retrieve emails according to specific criteria.

Introducing S/MIME email certificates from Sectigo

Sectigo is the leading provider of strong digital identities using public key technology. These identities are valuable for a wide range of applications in the enterprise, from mobile device authentication in wireless networks to encrypting and digitally signing emails using the popular S/MIME standard. For effective HIPAA compliance, email encryption must be invisible, easy for the administrator to deploy, and easy for the employee to use. Unfortunately, previous S/MIME solutions have been quite difficult, with the result that employees routinely fail to encrypt their email. This situation can lead to non-compliance even when a solution is in place.

To solve this problem Sectigo developed the industry's first, zero-touch, X.509 certificate management system. This system provisions digital identities automatically to any application using traditional Windows or mobile devices. Many popular mail applications support SMIME, so there is no need to change your systems or methods of working. Healthcare professionals will have the ability to exploit the convenience of their tablets and mobile devices using the same mail applications they use today.

A single administrator console allows for the provisioning of both publicly trusted S/MIME certificates and private certificates dedicated to the exclusive use of the enterprise. The console allows for control over employee, server, and device enrollment. It effortlessly provides discovery, reporting, automated renewal without employee involvement, and revocation when the employee leaves.

For enterprises the console automatically adopts all previously issued certificates to dramatically improve deployment. The administrator can choose to replace these certificates automatically with publicly trusted S/MIME certificates. Public S/MIME allows for any S/MIME-capable mail application to validate the both sender's identity and the fact that the email and its attachments have not been altered in transit. Furthermore, the email certificate enables the encryption of both the email body and its attachments, all with no change to the end user's email experience.

To truly enable nearly 100% of emails to be encrypted, the solution adds these important features ignored by previous S/MIME solutions:

- **Sending the entire encryption key history to all mails applications so even older emails can be decrypted**
- **Hosting of an LDAP directory to allow Health Information Exchanges to share certificates**
- **Encryption key archiving so employees can recover accidentally destroyed keys**
- **Interoperation with the secure email gateways (SEGs) so that the enterprise may still use mail scanners to perform their functions on encrypted and signed emails**

