

Passport 4000 SecurePort

SecurePort: The Passport 4000 Secure Email Interface

SecurePort helps the healthcare industry meet existing and emerging regulatory frameworks whilst improving the trust between customer and partner.

Since the introduction of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 and the more recent Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, healthcare providers are under ever increasing pressure to ensure the security of Protected Health Information (PHI). This security not only relates to PHI stored within the organisation but also to when it is electronically (e-PHI) transmitted outside of the organisation to other entities.

Since email is not a secure communications medium the transfer of e-PHI such as patient details and reports via email is open to all sorts of compliance breaches. Emails containing PHI could be sent to the wrong address or get intercepted and read by the wrong people. SecurePort offers a solution to these problems by providing a choice of secure delivery methods including PKI Encryption and password protection.

Once the method of communicating secure emails has been agreed with the customer then their profile is created within SecurePort and their associated certificate or password registered in the SecurePort store. When a document is generated from the healthcare system for delivery to email, SecurePort will validate that there is a secure transport method configured and that the associated security for that transport is in place before continuing to process and deliver the document.

To provide increased flexibility and simple customer migration paths, SecurePort can easily be added to your existing Passport 4000 fax Server in order to offer both fax and secure email delivery options to meet your customers' requirements.

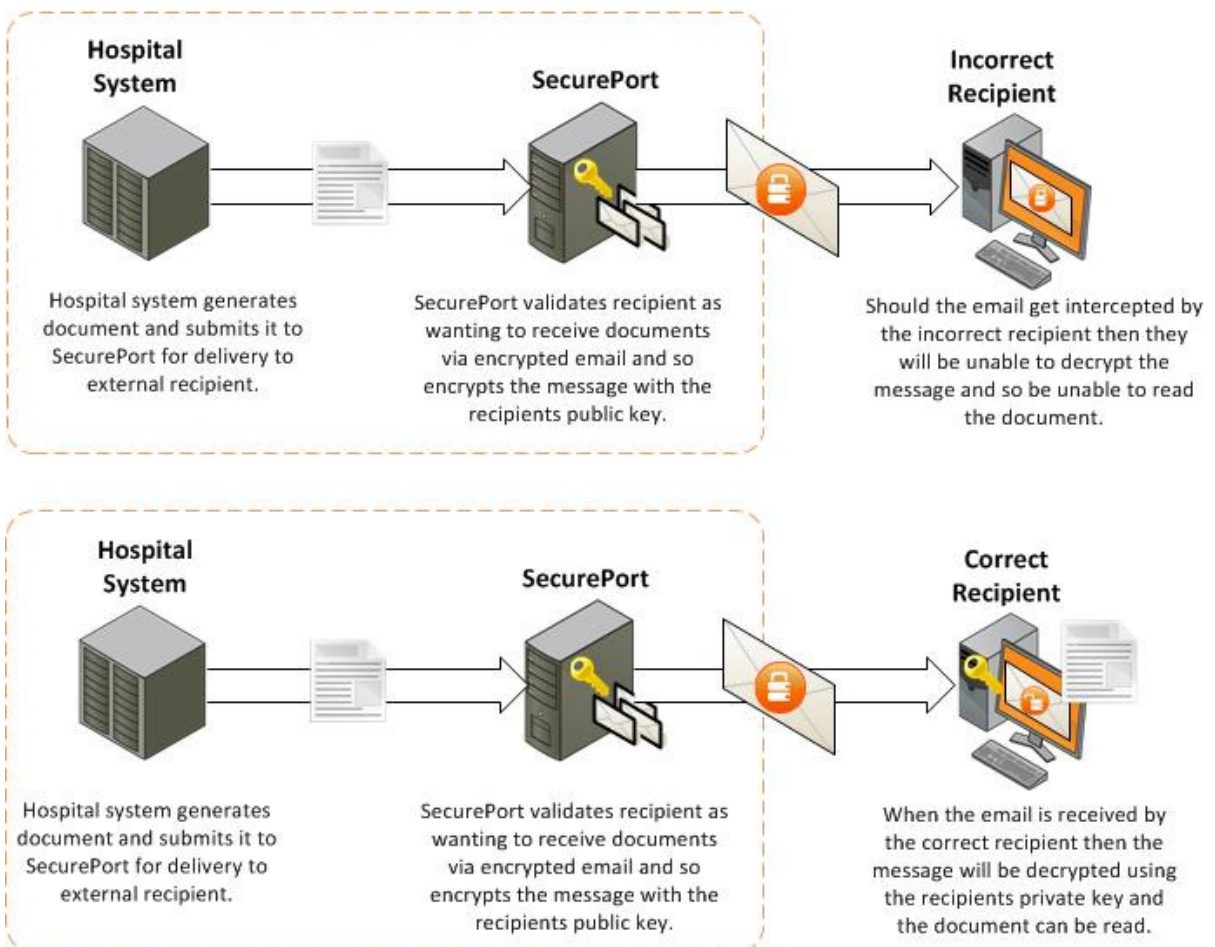
Transmission Security. *A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.*

THE HIPAA SECURITY RULE



Encryption - PKI security

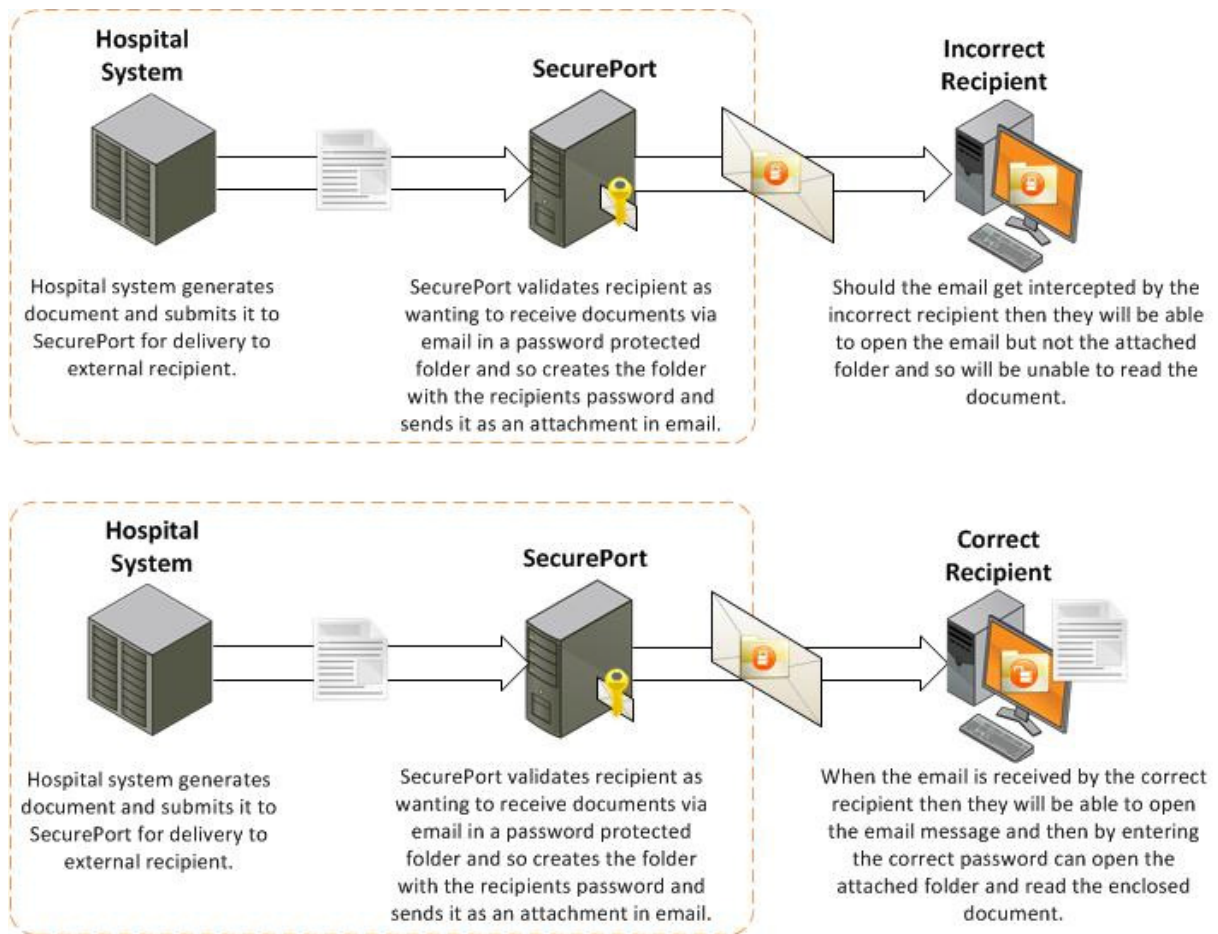
For maximum security the encryption option is recommended. The document is attached to an email which is then encrypted using the recipient's public key. The public key which is part of a trusted digital certificate is provided by the recipient and stored securely in the passport 4000 store. The encrypted email is then sent to the recipients designated email address. On receiving the email it can only be opened if the recipient is the owner of the corresponding private key that belongs to the same trusted digital certificate.



To enable encryption each recipient must provide their own PKI certificate. The recipient is responsible for obtaining their certificate from a trusted authority and they must then provide their 'public' certificate for registration within the Passport 4000 SecurePort server. Certificate registration can be performed automatically or manually.

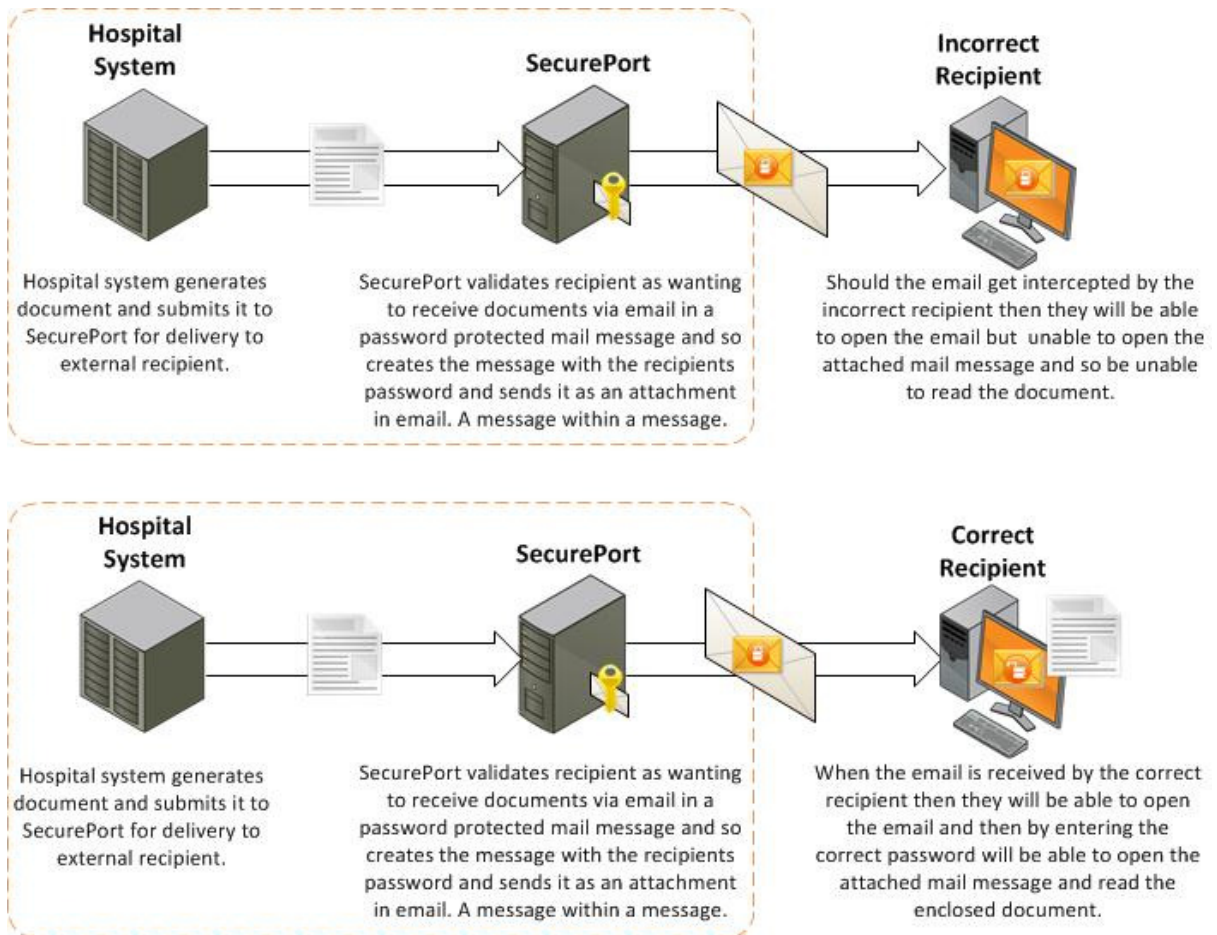
Password Protected Folder

A password-protected compressed “ZIP” folder attachment is created which contains the message body and all document attachments. The password is provided by the recipient and stored securely in the passport 4000 store. This password protected folder is then attached to an email and sent to the recipients designated email address. On receiving the email it can be opened but the password must be entered before the contents of the folder can be viewed. For extra security it is recommended that strong password techniques are used when choosing a suitable password.



Password Protected Email

A password-protected compressed “ZIP” Email Message file attachment is created which contains the message body and all document attachments. The password is provided by the recipient and stored securely in the passport 4000 store. This password protected email message is then attached to the main email creating a message within a message and sent to the recipients designated email address. On receiving the email the main message can be opened but the password must be entered before the attached email message together with its contents can be viewed. For extra security it is recommended that strong password techniques are used when choosing a suitable password.



North and South America
LANE Telecommunications, Inc.
Tel: +1 973 526 2979
Fax: +1 973 526 2988

United Kingdom and Europe
LANE Telecommunications Ltd.
Tel: +44 (0) 1256 301550
Fax: +44 (0) 1256 301555

Singapore and Asia
LANE Telecommunications, PTE.
Tel: +65 6353 0555
Fax: +65 6353 7448