E-mail Encryption – Client FAQs

Q. What is e-mail encryption?
A. E-mail encryption refers to the protection of information, making the message readable to only the intended recipient, and may also require the recipient to confirm his/her identity.

Q. Why is Concentra implementing an e-mail encryption program?
A. We believe that privacy and security are paramount, especially when it comes to sensitive and confidential personal information. As part of Concentra's commitment to provide outstanding service to clients, we're taking this proactive step to create an added layer of security, to protect the exchange of personal information.

Due to both state and federal legislation, certain personal information should only be shared through a secure network, which includes email encryption. In certain states, such as Massachusetts, these laws are already in effect, and Concentra is rolling out the system to be compliant.

Additionally, Humana's security and regulatory group has already implemented its e-mail encryption service, and Concentra is rolling out its own, in order to be compliant with Humana standards and operating policies.

Q. Will this encryption process affect everyone?
A. The encryption process will be automatically triggered any time a Concentra colleague sends potentially sensitive information to any external e-mail. This trigger will not be visible to Concentra colleagues, and takes place after an e-mail has been developed and sent. Colleagues should see no change in the view of e-mail messages.

Only e-mails that contain potentially sensitive information will be encrypted. Those without the select information will not be encrypted and will operate as normal, unless the sender forces encryption (see more below).

Q. What information will be encrypted?
A. Not all information will be encrypted, only e-mails that contain certain codes and information deemed as sensitive. This includes information such as social security numbers, national drug code classes, code dosages, code names, code routes, procedure codes, ICD-9 diagnosis codes, American Banking Association numbers, and credit card numbers.

Additionally, the sender can choose to encrypt the e-mail if there is confidential information that may not be included in these specific triggers, such as contract pricing agreements.

Q. Can secure accounts be verified before the rollout?
A. Yes. The e-mail security team will be working with sales reps and e-mail administrators at client companies to establish a TLS account for clients, prior to the roll-out. Sales reps can download a copy of the **Encryption Worksheet**, and contact Chris LeRoy to begin setting up the TLS connection for clients.

Q. What will encrypted messages look like?
A. Upon **first** receipt of an encrypted e-mail from Concentra, users will receive a notification of the encryption with a link to set up an account and password. Thereafter, recipients will receive the encrypted e-mail content as an attachment and will be asked for the user name and password in order to read the attachment. Following is an example of how this message may look.

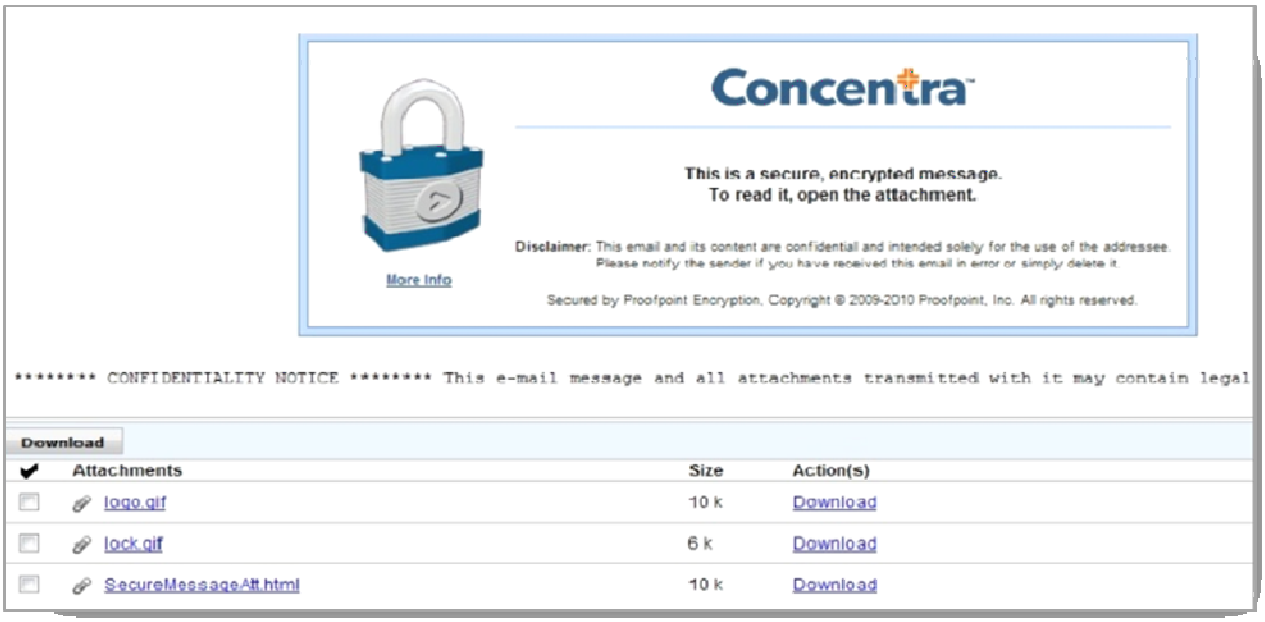

Image 1.

Q. How can recipients access encrypted e-mail information?
A. Upon **first** receipt of an encrypted e-mail from Concentra, users will need to establish a secure connection before being able to view the e-mail message. There are two ways this can be accomplished:

1. - Recipients can register their e-mail address, and create their own password within the encryption site in order to read the encrypted info. Step-by-step directions will be included in the first encrypted e-mail notification. This same information will need to be entered into the system each time a user wants to access and view encrypted information.

2. - A client company can receive sensitive information directly through e-mail, by setting up a TLS connection between your company's e-mail client and Concentra's e-mail system. Through the TLS connection, every member of your organization will be cleared to receive information without the need for each individual to create his/her own account and password in order to view the e-mail.

Q. Will attachments also be encrypted?
A. Encryption extends to the content in an e-mail as well as certain attachment formats that the encryption system can scan. If sensitive information is identified in a message, the body of the message, the attachment, or both may be encrypted.

10. Is there a way that clients can avoid this process?
Yes, clients can establish a business-to-business secure communications line, also known as a TLS, which will eliminate the need for accessing e-mails with a password. The e-mail security team will be working with sales reps and e-mail administrators at client companies to establish a TLS account for clients, prior to the roll-out. Sales reps can download a copy of the **Encryption Worksheet**, and contact Chris LeRoy to begin setting up the TLS connection for clients.

Q. Can a client respond back to an e-mail that contains sensitive information?
A. Clients can respond back to encrypted e-mails, as long as the communication string occurs between the original sender and recipient. Additionally, the recipient may add other names to a reply *if* those e-mail addresses use the same e-mail domain format. Additional recipients included in a reply that use a different e-mail format will not receive the reply.

Q. Can I send an e-mail that contains personal health information to multiple contacts?
A. An encrypted e-mail sent to multiple contacts will require each recipient to establish a secure connection. Each recipient will need to set-up his/her own account and password in order to view the content.

Additionally, encrypted e-mails cannot be read or accessed by clients who have an automated e-mail processor. Individuals will need to personally log-in to the encryption site, and confirm their identity with their password before viewing the e-mail content.

Q. Can I share an e-mail that contains personal health information with others in my organization?
A. Yes. E-mails that contain encrypted information can be forwarded to others within the same organization, so long as all e-mail domain formats are the same, i.e., everyone uses the same *firstlast@company1.com format*.

Q. What is Proofpoint?
A. Proofpoint is Concentra's official vendor for e-mail security and compliance solutions. Proofpoint's expertise, patented technologies and on-demand delivery system help organizations protect against spam and viruses, safeguard privacy, and encrypt sensitive information.

Q. What is TLS?
A. TLS stands for Transport Layer Security, and allows two entities to communicate across a secure network, helping to prevent eavesdropping and tampering of information. During the transmission of information, the sender's and recipient's systems agree to establish the connection's security. Companies who implement a TLS system create a company-wide auto-encryption process that makes individual recipient password authorization unnecessary.

Q. Where can I get more information about the encryption process and benefits?

A. You should work directly with your account representative to address any issues or concerns about the new e-mail encryption program. Your account representative can also help to connect your company's e-mail administrator with Concentra's e-mail administrator for any technical support issues, or to set up a TLS auto-encryption process.

Q. How long does an encrypted e-mail stay active?
A. Encrypted e-mails and attachments are stored within a recipient's own e-mail system, so encrypted message can be unlocked and reviewed indefinitely or as long as your own e-mail system maintains active files.

Q. Why do I get different screen images about the encryption link when using different systems?
A. Due to the varying e-mail platforms, certain systems will process images and layouts differently. This change does not affect the user's capabilities to access links to the encrypted e-mail or reply back to an encrypted e-mail.

Q. How does this new system change the reports I receive from Concentra?
A. Depending upon the information normally shared in your reports, you may now have to confirm your identity using the encryption password in order to access the reports. If you typically share your reports with other members of your company, the content from the encrypted e-mail will need to be saved and attached in a new e-mail, since encrypted e-mails cannot be forwarded.

Q. Will my information be shared to vendors/solicitors by Proofpoint?
A. No. All information verified by Proofpoint is strictly confidential, and will not be shared with any third-parties. The e-mail addresses and information therein are strictly used to ensure a secure information network is established.

Q. Will I be charged for this additional layer of security?
A. No. This additional layer of security will not result in any additional charges for clients. As part of Concentra's commitment to outstanding service to clients, we are taking this proactive step to protect the exchange of personal information.