Email Encryption

Frequently Asked Questions

What is email encryption?

Email encryption is the process of protecting the content of email messages (containing restricted confidential data) from being read by unintended recipients. By leveraging the Palomar Health's Proofpoint solution, which is responsible for scanning for spam and viruses, we are able to provide our users with the ability to send encrypted email whenever necessary.

Why and when should I encrypt email?

Use of Palomar Health's secure email system is intended to address the need for communicating restricted/confidential data (i.e. PHI) in a safe and secure manner and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, it can also be used to secure other sensitive information including, but not limited to, personal identifiable information (PII) or financial information. You are required to use secure email whenever you send a message that contains sensitive information such as PHI or PII to a recipient on the Internet. For guidance on the types of email that should be encrypted, please review the following Lucidoc Procedures for more information on encryption: (1) Computer System – 10341, (2) Email Access and Appropriate Use – 20310 (3) Data Encryption – 20730

What will happen to secure emails sent previously through Zix?

Email that was sent in Zix will still be available for retrieval from Zix, but all encrypted emails sent after August 25th will be in Proofpoint. You will be directed to the secure site pick up in Proofpoint at that time. The entirety of any emails that is sent before and after the transition period will be available in Proofpoint. Zix licensing for all users expires September 30, 2018.

Who will decide if my mail is encrypted?

Based upon the content you are sending; you make the decision about whether or not an email will be encrypted. **The email you send will only be encrypted if you include the word "Secure" is in the email subject.** The word secure will be read with a wildcard which means it can have parenthesis, brackets, quotes - any punctuation or letters prefixing or suffixing the word.

Can recipients reply to my messages securely?

Yes, recipients of your secure messages can reply securely by accessing the URL or attachment in the email they receive. Their reply to your email will be automatically decrypted by the secure email system and will appear in your Palomar Health mailbox as a normal, readable email. The process is seamless and the only indication that the message was originally encrypted will be the "[secure]" in the subject line.

Can business associates outside of Palomar secure messages to me?

Third parties can initiate an encrypted communication if they generate the email from their Proofpoint account portal. They are limited in that they must send to Palomar Health recipients only.

How will secure mail recipients receive encrypted messages?

Recipients of a secure email from Palomar Health will receive a notice in their email inbox that they have received a secure message from you. The message will contain an encrypted attachment or URL, which when opened, will take you to the secure email server. The first time the recipient receives a secure message, they will be asked to create a passphrase that will be used to view or reply to their secure messages. After logging in with their self-assigned passphrase, the recipient can then view the

email and use the "Reply" button to reply to the message. **Job Aid available on the Intranet under "E" for Email within the ProofPoint subheading**

Can I send a message while I travel?

Yes, you can send secure messages using the Outlook web access page located at https://webmail.palomarhealth.org. This website provides most of the functionality of regular e-mail. Again, an email will not be encrypted unless you place "secure" in the subject line.

Is the subject line of the message encrypted?

The subject of the email is **not** encrypted; therefore, you should not include sensitive information in the subject line.

Can I send attachments?

Yes, the total size of attachments you send must not exceed 15 megabytes.

Do I still need to encrypt emails to someone with a Palomar Health email address?

Encryption must always be used when Palomar Health Confidential Information is transmitted over electronic communications networks e.g. via e-mail. This best practice is to circumvent a scenario in which an outside email address is added onto the chain or the email is forwarded outside the organization. The encrypted email will send just like any other email to users with Palomar Health accounts but will pass through the Proofpoint secure email portal for any recipients outside Palomar.

How do I send secure email?

By simply putting the word "secure" in the subject line of your Palomar Health email, your message will be encrypted. The trigger for the word secure has a wildcard feature so regardless of how it's used within the subject line, if it appears, your email will be encrypted. **Job Aid available on the Intranet under "E" for Email within the ProofPoint subheading**

How long until the encrypted message expires?

Encrypted mail will be available for the recipient for 14 days

How long until my password expires?

Your password is linked to your Palomar network password and thus follows the same expiration timeline. Your proofpoint password will update automatically when you update your password through Palomar's Self Service Password tool.

How do I set up to use secure email?

All employees with a Palomar Health email account can use the secure email system. There is no pre-registration or setup required. Users outside the organization will have to sign into and register an account to view the message. **Job Aid available on the Intranet under "E" for Email within the ProofPoint subheading for individuals outside of Palomar Health initiating secure email to Palomar Health employees**

Questions about secure email not covered in the FAQ should be directed to Palomar Health Information Security at InfoSec@palomarhealth.org