

Lancaster General Health

Encrypted Email FAQ for Internal Users

Lancaster General Health has upgraded the encrypted email service. This service should be used whenever patient or sensitive information is to be delivered by email. Documentation is available on the LGHealth intranet.

Who is this document for?

This document is written for the user who is internal to the Lancaster General Health system. When you sign into your workstation, you are signing into the LGH network. Another way to tell is if your email address that you use for the bulk of your normal business correspondence is like one of the following:

- yourid@lancastergeneral.org
- yourid@lghealth.org
- yourid@lancastergeneralcollege.edu

Who can I send encrypted email to?

The encrypted email system only comes into play when you are sending email from your Lancaster General Health account, and are sending it to a recipient who is not a member of the LGH system. The system is meant to protect correspondence between LGH and our business partners, vendors, and customers.

What is the difference between regular Email and Encrypted Email?

Almost all email is sent “in the clear” over the Internet. If someone were to intercept an email you have sent, before it arrived at its intended recipient, that person could easily read your entire email. An encrypted email service makes sure that even if the email is intercepted, it would be unreadable by anyone except the person for whom it was intended.

Why should I encrypt e-mail?

Lancaster General Hospital is committed to protecting the privacy and confidentiality of our patient's information. The policy, “*ELECTRONIC MEDIA SERVICES AND CONFIDENTIALITY*” clearly states:

Encryption Requirements:

- Internal email is considered secure; therefore, sensitive information may be transmitted internally without encryption.
- Internet Email is not secure. Protected Health Information (PHI) may not be transmitted over the Internet without approval from the Director, Clinical Information Management. All PHI sent externally must be encrypted prior to transmission.
- Other sensitive business information sent via the Internet or Internet Email must also be encrypted. The owner of the information will make the decision on whether the information is sensitive. (e.g. sensitive Employee information determined by VP, Human Resources)

Lancaster General Health Encrypted Email FAQ for Internal Users

- Encryption will only be accomplished using products/procedures approved by the Manager, Information Systems Security. **Note:** Password protecting a file is NOT considered encryption and may not be used as a means of protecting sensitive data.

When should I use Encrypted Email?

You should encrypt email when you are sending information that is sensitive or protected.

Any transmission of patient information must be cleared **first** by the Director, Health Information Management. This would include individually identifiable health information, referred to as "Protected Health Information" (PHI).

Encrypted Email is available if you are sending other sensitive information such as legal or financial communications. Check with your supervisor if you have a question.

Also, be mindful of the size of the material you are going to Email. If the material is very large (greater than 10Mb), consider creating a CD of the material and using ground mail to deliver the information.

Who will decide if my mail is encrypted?

If you are internal to the Lancaster General Health System and starting in June of 2010, a system will be in place that will evaluate the contents of outgoing email, and make a calculation, based on content, on the likelihood of the email containing patient information or sensitive information. Based on that decision, the system will mark the email for encryption and continue processing.

So Why Should I Encrypt, If the System is Doing It?

If you know that the information is sensitive, please continue to mark the email for encryption. The decision making process for automatically encrypt and email is statistical, and very similar to the anti-spam filter.

Also, manually requesting email encryption cuts down on the amount of processing the encrypted email system has to do in order to process your email.

How do I encrypt messages?

The message must be sent from inside of the LGH network. This means that you must be at a workstation here at the hospital, or signed in to OWA.

Add the phrase "lg-secure" to the subject line. The subject of your e-mail message might look something like this. *lg-secure lab report*. Putting the phrase "lg-secure" anywhere in the subject line will encrypt the message. Please do not include sensitive information in subject line of the email, since the subject will not be encrypted.

Lancaster General Health Encrypted Email FAQ for Internal Users

Can I send Encrypted Email to anyone?

Yes, but there are some requirements:

1. The recipient must have access to the Internet (that is, they should be able to see www.google.com or www.cnet.com, etc. from their web browser).
2. The recipient's workstation should also have JAVA installed. The recipient should check with their own Information Services group to check on this.
3. They must be registered in the system, first. There is a link on the encrypted email that will allow a first time user to register. There is also an explanation in the detailed documentation in the Intranet Help Desk document.

The system is for transferring sensitive information and ePHI. It is not intended for personal use.

How will secure mail recipients receive encrypted messages?

When you send an encrypted email, the recipient will receive a **notification** in the email that an encrypted message is waiting for them.

There will be an HTML attachment that your recipient will always be able to decrypt, along with a link to the LGHealth web site that will provide a web email interface for one week to the same email. Reading either will require that the recipient be registered in the system, and authenticate before they can read their email.

There are some locations that will strip out the HTML attachment. If your recipient is one of these, they will still be able to use the web based email server, and read it there for one week.

Can users reply to my messages securely?

Yes, your email recipients will have the chance from your encrypted email to send a secure reply. They can even send attachments back with their reply. Details can be found on the Help Desk document.

How can I make sure my messages are being encrypted? Can I test the system?

We encourage you to familiarize yourself with the system by sending encrypted messages to your business associates. It will be very easy to tell if the message was encrypted because recipients will have to register their e-mail address and use a password to access the message. Details can be found on the Help Desk document.

Lancaster General Health Encrypted Email FAQ for Internal Users

Can I encrypt messages sent to other Lancaster General e-mail address using the Lancaster General Encrypted Email system?

NO, e-mail messages sent to other Lancaster General e-mail address (that is, email address that you get out of the global address book in Outlook or OWA) will not be encrypted. Only e-mail **leaving** the Lancaster General network for the internet can be encrypted with this system.

What if I forget my Password?

The system will allow you to reset your password. You must answer 3 of the 5 challenge questions in order to reset your password. You will have to type in your answers the way you originally put them in, as upper and lower case matter.

If you forget your challenge answers, your password can also be reset by the system administrator of the service.

I marked an email for encryption and my recipient says that it arrived in the clear! What happened?

There's a new feature that we've implemented with the Lancaster General Health encrypted email system, and it takes advantage of a feature that's available with more modern mail delivery systems. Instead of encrypting the mail message, two mail servers will set up an encrypted pipe between themselves, and deliver mail through that. Your email has been sent protected, but the recipient does not need to register in the LGH secure email service. If your recipient is interested in this kind of service, have them talk to their own IS staff about setting up 'TLS mail delivery', or have them contact LGH/Information Services for more information.

Where do I go if I need help?

You can do one of several things if you are a recipient and run into trouble:

1. Call operations (717 544 5001 – Option 2). Tell them you are using the encrypted email system and are having difficulty.
2. Get in touch with the sender. Have them open a ticket in the IS request ticketing system. That is what operations will do.

There is no support out of business hours (8am to 5pm). Support will be provided within one business day or sooner.