

BryanLGH Medical Center

Secure E-mail FAQ

What is Secure E-mail?

The most popular form of security relies on encryption, the process of encoding information in such a way that only the person (or computer) with the “key” can decode it.

Another process, authentication, is used to verify that the information comes from a trusted source. Basically, if the information is “authentic,” it is known who created it and that it has not been altered in any way since that person created it. These two processes, encryption and authentication, work hand-in-hand to create a secure E-mail environment.

How does Secure E-mail work?

We have contracted with a company, ZixCorp, to screen all outbound E-mails. A process is used to scan the content of the E-mail and all attachments for words that can be construed as protected health information (PHI). If one word or more is found, the E-mail is encrypted. This DOES NOT affect E-mail sent internally. For example, if you send E-mail to another BryanLGH Medical Center employee address, screening is not required.

If you send an outbound message that matches a PHI pattern, the recipient will receive an E-mail message telling them that a confidential message is waiting for them at a secure Web location.



**Welcome to BryanLGH Medical Center
Secure Email Message Center**

Email Address:

Password:

Useful Links:
[Forgot your password? Change your password](#)
[Forgot your password? Send a password reminder](#)
[Register for a new account](#)
[Use online help](#)

For Customer Support, email us at support@zixcorp.com.

Example of Secure Message Center

To pick up the message from our Secure Message Center, the recipient will click on the link provided in the notification E-mail. They will then link to a Password Creation screen. The recipient enters his/her E-mail address and then creates a password. They must remember the password, as they will use it each time to log into our Secure Message Center. The password must be at least six characters long AND contain one or more numbers OR include both upper and lower case letters.

BryanLGH Medical Center

Secure E-mail FAQ

Why is Secure E-mail necessary?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires BryanLGH Medical Center to provide a secure method of delivering Protected Health Information (PHI), such as a patient's name, address, phone number, medical terminology and/or information about the patient's specific health insurance coverage via E-mail.

Because we respect the privacy of both our patients and our network of hospitals, doctors, and other health care professionals and in an effort to comply with the HIPAA guidelines, BryanLGH Medical Center will implement an additional layer of electronic mail security.

When will Secure E-mail begin?

The effective date is December 30, 2003.

What types of words are screened?

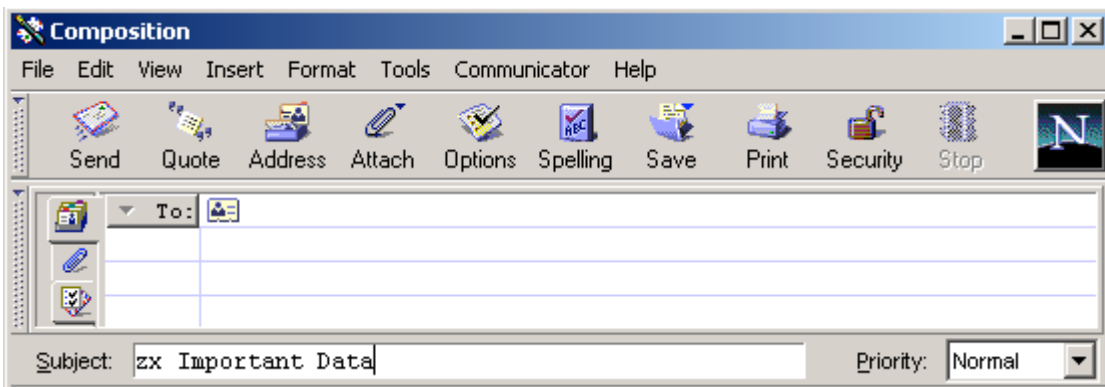
Zixcorp uses common lexicons, or a dictionary of words, to scan both the content of the E-mail and any attachments. These words are determined by ZixCorp and cannot be changed by BryanLGH.

Words such as admit date, month abbreviations, account number, disease names, family titles (mom, brother, etc), diagnostics, HCPCS, general conditions, substance abuse, mental health, medical record information and claims will cause E-mail to be encrypted. At times, the service will encrypt messages that match a PHI pattern but do not actually contain PHI data.

To assure encryption, always type zx followed by a space and then your subject in the subject line of your E-mail. You may use capital or lower case letters.

How do I force my document to encrypt?

At times, there may be a document that you would like to remain confidential. Documents that contain employee or legal information should be encrypted. To force a document to encrypt, type the letters zx followed by a space and then your subject in the subject line of the E-mail. You can also type the letters zx at the beginning of the text in your e-mail. DO



NOT PUT PHI DATA IN THE SUBJECT OF THE E-MAIL.

Example of how to force encryption using the subject line

Why did I receive an E-mail notice from Zix stating that my E-mail is not deliverable?

BryanLGH Medical Center Secure E-mail FAQ

Read the contents of the E-mail to determine why the message is undeliverable. It may be that you mistyped the E-mail address. It could also be that the subject of the E-mail contained PHI data. Since the subject itself is not encrypted, the E-mail will not be delivered if it contains PHI in the subject. For example, if the subject contains a person's name, a series of numbers or a medical term, the E-mail will be returned to you.

How long will Zix keep the E-mail I've sent?

The E-mail will be available to the recipient for 21 days. If the recipient does not view the E-mail within that time, it will be removed from viewing and you will receive an E-mail notice stating the unread E-mail has expired.

How can I find out more information?

Computer/Technical Questions	IT Help Desk	18960
HIPAA Related Questions	Karen Adamsheck, Compliance Coordinator	18961 481-8961
Secure Message Center	http://www.zixcorp.com/support/faq_zmc.php	

How will we know if this is effective?

BryanLGH Medical Center will conduct a survey of all incoming and outgoing E-mails soon. This will help us to determine if the lexicons we use are accurate and to monitor E-mail traffic.