

## **Information Security**

### **Secure Messaging:**

#### **Frequently Asked Questions for OHSU Personnel**

1. What is e-mail encryption?

E-mail encryption means that information in an e-mail as well as email attachments are scrambled or coded so that other people (for example, computer hackers or identity thieves) can't read or intercept information while it's traveling over the Internet.

2. Who can encrypt e-mails?

Anyone with an OHSU computer account and Microsoft Outlook access can encrypt e-mails. In order to use OHSU's encryption technology, you must use Outlook.

3. Why should I use encryption?

Encrypting information when it's e-mailed to addresses outside of OHSU helps to keep this information from being intercepted, viewed, or stolen by people who do not have a right to it. See the next question for examples of types of information that should be encrypted.

4. When should I use encryption?

You should use encryption when you are sending sensitive information to an e-mail address OUTSIDE of OHSU's network. If someone's e-mail address does not end in ohsu.edu, it is outside of our network. Some examples of sensitive information are:

- \* Protected health information (PHI)
- \* Certain OHSU financial data
- \* Intellectual property
- \* Certain research data
- \* Proprietary information

Sensitive information sent to e-mail addresses INSIDE our computer network (e-mail addresses ending in ohsu.edu) is already secure and does not need to be encrypted.

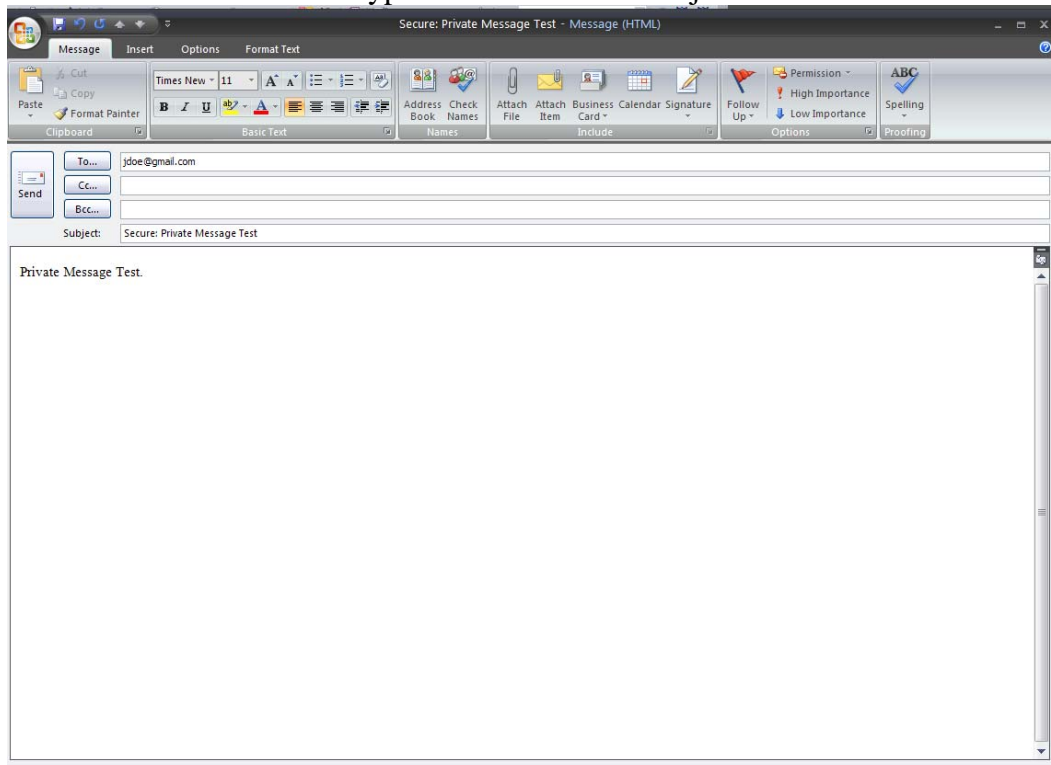
There are some cases when you MUST encrypt sensitive information sent to e-mail addresses that are outside of our network. One example would be e-mailing protected health information (PHI) to a health care provider who is outside of OHSU. In this case, HIPAA regulations require encryption of this information. If you have questions about when to encrypt e-mail, you can send an e-mail to oips@ohsu.edu requesting more information. However, a good rule of thumb is, if you're not sure if information you're e-mailing should be encrypted, encrypt it. When in doubt-Encrypt.

5. How do I encrypt an e-mail? There are two ways you can encrypt an e-mail.

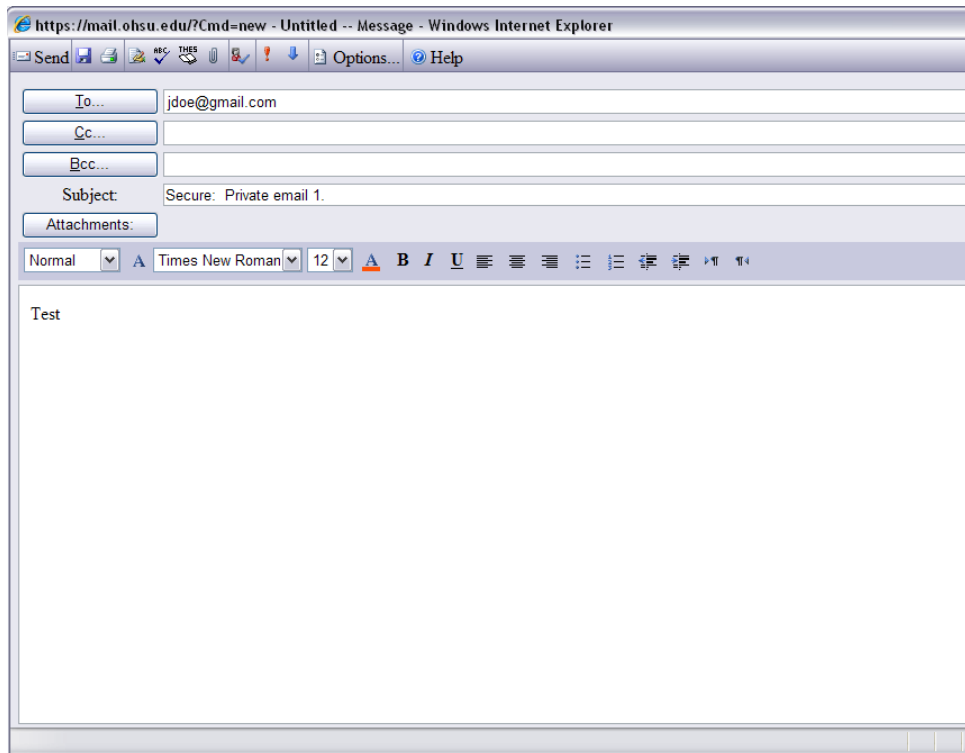
A. You must be using Microsoft Outlook or Outlook Web Access. Type Secure: as the first word in the subject line of an e-mail. You should not use quotes around the word secure and you must put a colon and a space directly after the word. It does not matter if you type SECURE: Secure: or secure: In other words, capitalization does not matter. After the colon and space you can fill in

an appropriate subject description. This option works for both PC and Macintosh users. See the picture below for what this would look like:

For the full Outlook client type **“Secure:”** in the Subject Line



For [Outlook Web Access](#) type **“Secure:”** in the Subject Line



### **Encrypting an e-mail secures both the e-mail text and any attachments.**

#### 6. Can I turn encryption off?

E-mail encryption is not turned on unless you use one of the methods described above. So, e-mail encryption is always turned off until you choose to turn it on.

#### 7. How will encryption change e-mail within OHSU?

E-mail encryption should not change anything for e-mails that are sent to addresses that end in ohsu.edu. If you send an encrypted e-mail to an address outside of OHSU (such as jane.doe@hotmail.com), the recipient will need to go to a web site and register in order to retrieve the e-mail you sent. For more information for encrypted e-mail recipients, see <http://www.ohsu.edu/xd/about/services/integrity/ips/resources/upload/Secure-Messaging-FAQ-s.pdf>

#### 8. What if the recipient has problems retrieving the e-mail?

The recipient will automatically receive instructions on how to retrieve their encrypted message. These instructions include information on what to do if they experience problems.

#### 9. Are there times when I should definitely NOT use encryption?

Encryption should NOT be used to send out messages to a listserve. From a technical perspective, if members of a listserve were all sent an encrypted message, they could only retrieve it by sharing the same account and password. This practice is not secure, and so defeats the purpose of encryption. Please do NOT use encryption when sending e-mail to a listserve. If someone on a listserve needs to receive a secure message, it should be sent individually to their e-mail account.

