Health Information & Technology | Security

November 1, 2018

Data Loss Prevention FAQs

Q: What is Data Loss Prevention (DLP) and what does it do?

A: DLP is a suite of software and hardware that is designed to help organizations protect data and prevent possible data leaks.

DLP has the ability to analyze, monitor, flag, encrypt and block data that contains sensitive or confidential information. This includes data stored within the internal Health System network and also data leaving the Health System network.

Q: Does this mean that all email is being monitored?

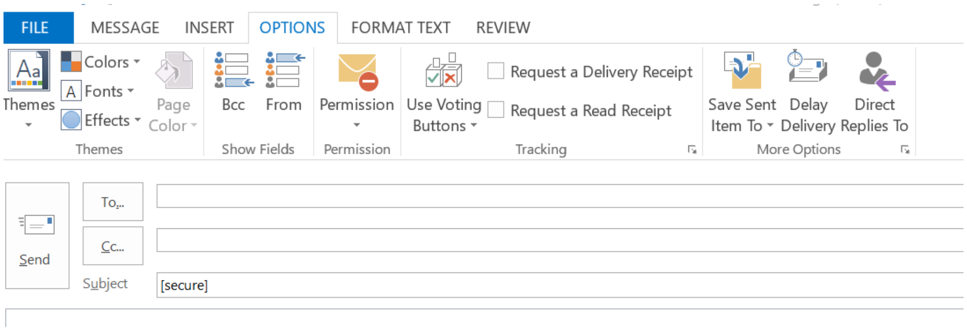
A: Email sent from a Health System (HS*) email account passes through the DLP server. If DLP determines that the message contains sensitive or confidential information such as patient identifiers or Security Numbers, etc., DLP will flag the email and a member of the DLP Response Team will investigate and follow up with the customer as needed.

Q: How can I encrypt my own email?

A: You may encrypt email by adding [secure] to your subject line or by using the confidential flag in Outlook.

Adding [SECURE] to subject line

1. Open a new email
2. Include [secure] in the email subject. Please be aware you must include the brackets and the word secure for the email to be encrypted. An email that contains [secure] in subject line will be encrypted before leaving the Health System network. Please be aware you will need to add [secure] to the subject line each time you send an email that contains confidential or sensitive information.

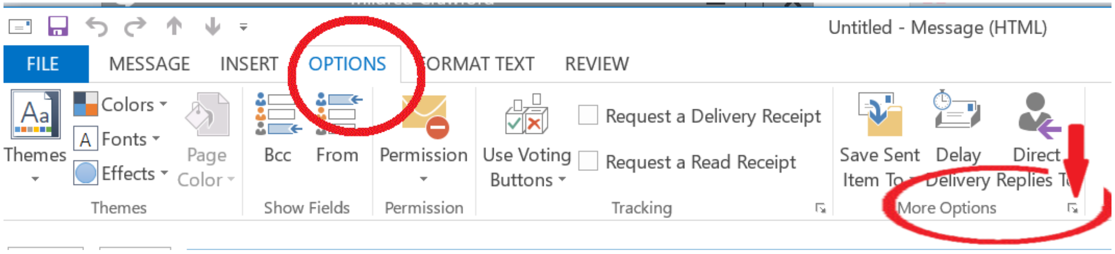


Subject [secure]

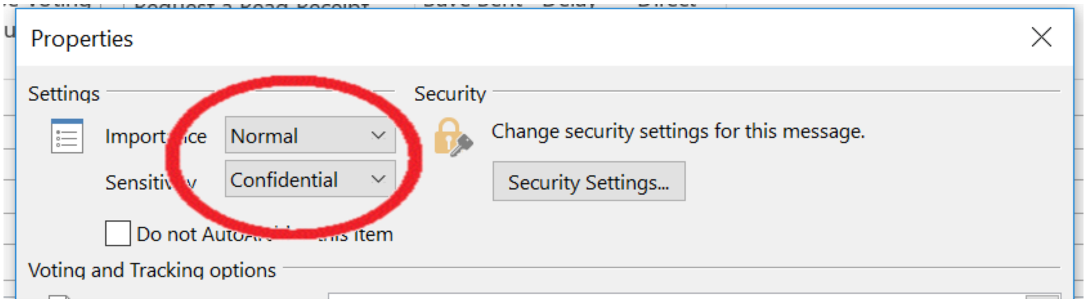
November 1, 2018

Setting Confidential Flag in Outlook

1. Open a new email
2. Click on the Options Tab
3. Click on the arrow beside More Options



4. Under Settings; Sensitivity click on the down arrow and select Confidential


Properties
Settings
Security
Change security settings for this message.
Security Settings...
Do not AutoArchive this item
Voting and Tracking options

Importance: Normal

Sensitivity: Confidential

6. Click Close

Q: When an email has been encrypted how will the email look to the recipient?

A: A sample of the email the recipient will receive is included below.

Q: I marked an email for encryption using the confidential flag or the keyword[secure]in the subject line and the recipient received the message rather than a notice. Why?

A: If the partnered organization uses the same email encryption solution as the Health System, then the email encryption is invisible to the recipient. Since there is no quick way to determine if a company is uses the same email encryption solution it is required that you send emails that contain sensitive or confidential information with [secure] in the subject line or with the confidential flag in Outlook selected.

Q: Why did I receive a BLOCKED TRANSMISSION notification when I attempted to visit a legitimate website?
A: You received the notification because you attempted to transmit sensitive or confidential information. Examples of sensitive and confidential information are Protected Health Information (PHI), employee data or financials.

Q: Who should I call when I have received a BLOCKED TRANSMISSION notification?
A: Please contact the HIT Helpdesk at 434-924-5334 or email the HIT Information Security Office at MCCSecurity@hscmail.mcc.virginia.edu.

Q: Who should I contact if I have questions?

A: You may contact the HSTS Helpdesk at 434-924-5334 or email the HSTS Information Security Office at MCCSecurity@hcsmail.mcc.virginia.edu.