ENCRYPTED EMAIL

The improper use or disclosure of sensitive information presents the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to students, faculty, staff, patients, and the University. Breaches of information privacy can also result in criminal and civil penalties for both the University and those individuals who improperly access or disclose sensitive information, as well as disciplinary action for responsible UT Health employees.

This document will help you determine which data is considered protected health information (PHI) and how you should send PHI data over e-mail.

Contents

Document Created on:	10/01/2016
Document Created by:	Salman Khan, Manager IT Security
Last modified by:	Salman Khan, Manager IT Security
Last modified date:	12/11/2017

Protected Health Information

Pursuant to HIPAA, individually identifiable health information collected or created by a covered entity is considered "protected health information," or PHI. University departments that use or disclose PHI are governed by HIPAA.

PHI is generally defined as:

Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

Employees should only access PHI only when it is necessary to perform their job-related duties.

Any of the following are considered identifiers under HIPAA:

- Patient names
- Geographic subdivisions (smaller than state)
- Web URLs and IP addresses
- Full face photographs or images
- Biometric identifiers
- Certificate/license numbers
- Vehicle identifiers
- Account numbers
- Telephone / Fax numbers
- Social Security numbers
- Dates (except year)
- Healthcare record numbers
- Device identifiers
- E-mail addresses
- Names of relatives
- Health plan beneficiary numbers

Any other unique number, code, or characteristic that can be linked to an individual

Individual Responsibilities

UT Health believes protecting our PHI is everyone's responsibility.

Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others) and work areas

Limit accidental disclosures (such as discussions in waiting rooms and hallways)

Include practices such as encryption, document shredding, locking doors and file storage areas, and use of passwords and codes for access.

Change passcodes frequently and keep them complex.

E-mail Encryption

Encryption is required when a University employee sends or receives PHI or PII. Encrypting your email may sound daunting, but it's actually quite simple.

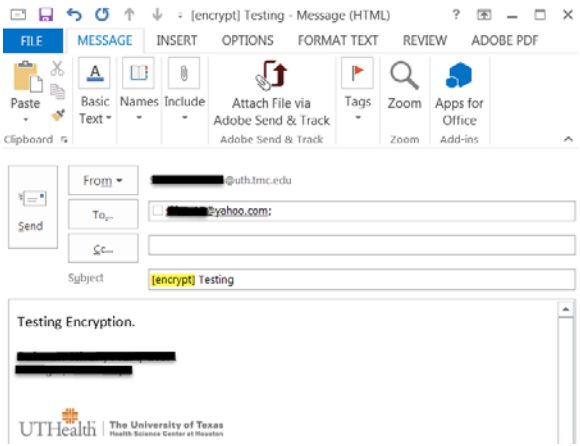
Sending Encrypted e-mails

Sending encrypted email to parties outside of the UTHealth network should only be done on an infrequent basis. If you find yourself needing to send e-mail containing PHI on a frequent basis please contact your LAN Manager to determine a better solution to your needs.

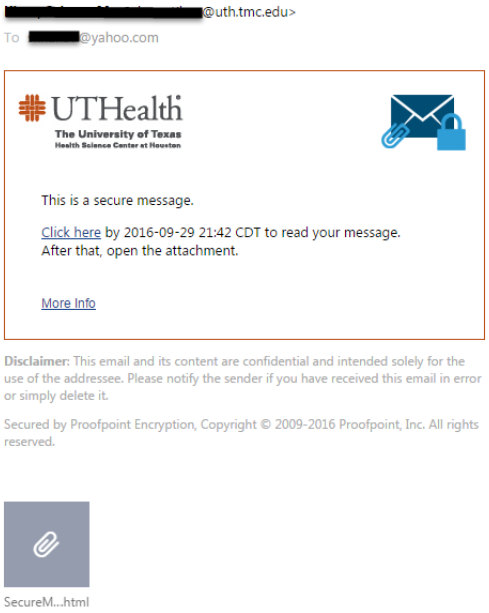
Encryption outside our network uses a tool called Proofpoint developed by CISCO. Proofpoint using a public and private encryption method so only the receiver of your e-mail can open it.

From within outlook or webmail in the subject line you must start the subject with "[encrypt]". **Never include protected health information (PHI) or non-public information in the subject line of your message**. Please remember that even if you choose to encrypt your message, any information in the email subject line will not be encrypted. If you're emailing medical records, for example, keep the patient's date of birth out of the subject line.

Type your e-mail as normal and then click Send as shown below:



Your email will shows up in the recipient's inbox and will look like this:



The first time the recipient of the message receives an encrypted e-mail from UTHealth, s/he will have to register with the Proofpoint system and set a password before s/he is able to read the encrypted message. Subsequent access to encrypted e-mails from UTHealth will just require the password that was originally set. If the user forgets the special Proofpoint encryption password for UTHealth, the "Forgot Password" link can be used to reset it. **Encrypted e-mail expire after 30 days. Encrypted e-mail also cannot be forwarded to other recipients.**

Proofpoint encrypted emails can only be opened on iOS mobile devices currently. If you are using another mobile phone operating system you will need to use Webmail (webmail.uth.tmc.edu) to open the email. Webmail can be opened using any phone's browser.

IT Security Recommendation / Guidance

- Send PHI via e-mail only as a last resort. Most UTHealth systems have secure messaging within the application to send PHI that ensures additional safeguards are met.

- Try to utilize share accounts that are approved by the University to share PHI. Google has an agreement in place with the University to store PHI information and can be a solution, if utilized properly to share PHI data.

- Always consider the audience before sending any PHI. Limit the PHI data to only that requested or needed.

Disclaimer

Proofpoint removes file attachments if the extension ends in the following:

Extension equals: "386" or "3gr" or "add" or "ade" or "asp" or "bas" or "bat" or "chm" or "cmd" or "com" or "cpl" or "crt" or "dbx" or "dll" or "exe" or "fon" or "hlp" or "hta" or "inf" or "ins" or "isp" or "js" or "jse" or "lnk" or "mdb" or "mde" or "msc" or "msi" or "msp" or "mst" or "ocx" or "pcd" or "pif" or "reg" or "scr" or "sct" or "shs" or "shb" or "url" or "vb" or "vbe" or "vbs" or "vxd" or "wsc" or "wsf" or "wsh"

This is to minimize potentially downloading malicious software.

- It is not possible to opt-out of executable attachment deletion.
- In addition to deleting based on file extension, Proofpoint will analyze the content and delete executables regardless of the extension.
- Proofpoint will look inside archives (e.g., tar, gzip, zip) and delete executable files.
- Deleted attachments are not recoverable.