Encryption

1. **Why has the encryption requirement changed?**

   When Yale first began to require encryption for devices within the HIPAA Covered Entity, we limited the requirement to those devices for which the user self-identified as creating, storing, accessing, transmitting or receiving PHI. We did this to protect the privacy of patient data. Some older machines experienced issues with the encryption software available at that time. Since that time, encryption software has improved to the point that it has minimal impact on user experience. As it is no longer burdensome for most devices to be encrypted, the University decided to require encryption more broadly thereby protecting University data, including PHI, intellectual property and Personally Identifying Information (PHI).

2. **Why is encryption necessary if I do not maintain PHI on my computer?**

   Our experience has shown that self-identification of computers containing PHI is inadequate in identifying all devices within the HIPAA Covered Entity that house PHI. We believe that there are several reasons including:

   - Misunderstanding of what constitutes PHI. HIPAA defines PHI very broadly and we have encountered many instances where users did not believe they had PHI as they had forgotten that dates associated with patient data render that data to be considered PHI under HIPAA.
   - The open environment of an academic medical center encourages sharing data, including data with PHI. For example, presentation slides that include PHI may be shared across an entire department, including individuals who otherwise wouldn't have access to PHI; or a data set may be shared with a colleague for discussions of data analysis or interpretation leading to PHI to be transferred to a device which wouldn't normally store PHI.
   - Devices are frequently re-purposed leading to a device being used to create, store, access, transmit or receive PHI that was not configured to do so as it was initially used for non-PHI purposes.
   - Human error leads to PHI being sent incorrectly to a device that was not adequately secured for that purpose.

3. **What does encryption do?**

   Encryption protects the data on your device in the event that the device is lost or stolen. Encryption scrambles the information on a device so that is unreadable to anyone who does not have the correct encryption key. Thus when an encrypted device is lost or stolen, the data remains inaccessible and confidential.

   Note: Laptop theft is the number one crime on the Yale campus per the Yale Police Department.

4. **Who is required to encrypt their computers?**

All devices used by faculty, staff and trainees of the HIPAA Covered Components or used by those who work on behalf of one of the HIPAA Covered Components of the University must be encrypted. The HIPAA Covered Components are:

- School of Medicine - excluding the School of Public Health, the Animal Resources Center, and the basic science departments: Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, and Pharmacology
- School of Nursing
- Yale Health
- Department of Psychology clinics
- Benefits Office

5. **What devices must be encrypted?**

   The requirement pertains to all devices that could be used to create, store, transmit or access ePHI including desktop computers, laptop computers, tablets, smartphones, thumb drives (USB), external hard drives, DVD's, etc.

6. **Won't encryption slow down my device?**

   No. In most cases, encryption will have minimal impact on device performance. Current software such as Bit Locker (MS Windows and File Vault 2 (Apple) are now standard on most new computers and laptops and have not been found to negatively impact performance.

7. **Can I set up the encryption myself?**

   No. Yale policy requires that centrally managed encryption be adopted. Additionally, Yale has the ability to set up the encryption with an "administrative key" which allows recovery of the data in the event you are unable to unlock the encryption. For example if you forget your encryption key, if Yale has configured the encryption on your device, IT staff would be able to implement the secure administrative key to provide access to your data. Without this administrative key, all data on the device would be lost if you forgot your encryption key.

8. **Is an exception possible**?

   Yes. The policy allows exceptions requests to be reviewed by the Chief Information Security Officer and where appropriate grant an exception. Exceptions based on legitimate business reasons are expected to be very limited however and will necessitate implementation of other methods to mitigate risks associated with having an unencrypted device. For example computers associated with specialized medical equipment/software may not be able to be encrypted. In such cases, enhanced physical security such as locking cables and/or locked rooms may be appropriate alternatives.

E-mail auto-forward

9. **Can I forward my email to another email address?**

   - Automated email forwarding, where all email is transferred to another email address is only allowed to addresses within the Yale-YNHHS networks (including yale.edu, ynhh.org, bpth.org, greenwichhospital.org).
   - Forwarding of limited emails based on specific criteria which would not lead to PHI being forwarded to a non-Yale or YNHH email account is also allowed. For example, setting a rule whereby email from an employee's child's school system is forwarded to a personal account is allowed.
   - Automatically forwarded all email to a non-Yale, non-YNHH account is expressly prohibited as the email is not secure in transmission and may not be stored securely on the host email system. The prohibition includes commercial email such as gmail, Yahoo, etc as well as email systems of close affiliates such as va.gov and ct.gov etc.