UW Medicine
SCHOOL OF MEDICINE

HIPAA Privacy and Security: FAQs

1. Use of paper case/procedure log books or papers (e.g., CORES reports) containing PHI or PII (personally identifiable information)

Q: What is the best practice regarding PHI/PII?
A: The best practice regarding PHI/PII, whether it is in paper, electronic or stored on a mobile device is to not take it off-site. PHI/PII should be stored in a locked drawer or cabinet. See below for security requirements.

Q: Can I leave my case/procedure log book or papers containing PHI locked in my car or the trunk of my car?
A: No. You cannot leave your log book or papers with PHI in your locked car or trunk. You must keep anything containing patient information in your physical possession during transit. You may not leave it unattended or in any mode of transport (even if it is locked).

Q: Can I leave my case log book or papers with PHI in a locked room at my home?
A: No. In order to properly secure these items, you must lock them in a safe or locked file drawer or cabinet in your home.

Q: After I have loaded the information into a computer system, what should I do with the paper containing PHI?
A: You must either shred the paper or place in secure recycling.

2. Use of mobile devices or laptops to store PHI/PII or case log information (Security)

Q: What is best practice regarding the use of mobile devices and laptops for storing PHI/PII?
A: Protection of confidential information is of the highest priority in UW Medicine. Confidential information includes PHI (protected health information) and PII (personally identifiable information). If possible, avoid storing PHI or PII on laptops, USB memory sticks, flash drives, iPhones or other mobile devices since any information on a mobile device is at higher risk of unauthorized disclosure due to theft or loss. If storage of PHI/PII on a mobile device is necessary, UW Medicine requires that the device be encrypted. We also strongly recommend that you enable the autolock function and remote wiping on mobile devices.

Q: What is encryption?
A: Encryption is the process of converting data into an unreadable format which is reversible with the use of a security key or password.

Q: Whose responsibility is it to ensure that the data or device is encrypted?
A: If you are storing PHI/PII on a personal or department-provided laptop or mobile device, it is your responsibility to ensure that the data stored on the device is encrypted.

Q: Where can I obtain information about encryption standards?
A: The UW Medicine Information Security Program has encryption information on their website: http://security.uwmedicine.org/security_tools/laptop_mobiledevice_encryption/default.asp

If you need information or help with encryption, contact ITServices Help Desk at mcsos@u.washington.edu. For urgent issues, call 206-543-7012.

Q: How do I enable the autolock function on my mobile device?
A: There are a number on online resources for assistance in configuring autolock on your phone:

- Apple's guide for iOS devices:
  http://support.apple.com/kb/ta38641

- Google's guide for Android:
  2.3 devices:
  http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/help/hc/pdfs/mobile/AndroidUsersGuide-2.3.4.pdf
  3.0 devices:
  http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/help/hc/pdfs/mobile/AndroidUsersGuide-30-100.pdf
- Microsoft's guide for Windows Phone devices: http://www.microsoft.com/windowsphone/en-us/howto/wp7/basics/lock-screens-faq.aspx

Q: How do I enable remote wiping on my mobile device?
A: Apple's guide to remote wiping an iOS device:
http://www.apple.com/iphone/built-in-apps/find-my-iphone.html
Google's guide to remote wiping an Android device:
http://www.google.com/support/a/bin/answer.py?answer=173390
Microsoft's guide to remote wiping a Windows Phone device:
http://www.microsoft.com/windowsphone/en-US/howto/wp7/basics/find-a-lost-phone.aspx

Q: Where can I obtain security awareness training?
A: As a member of the UW Medicine workforce, you are responsible for protecting UW Medicine systems and data. General Security Awareness (GSA) training is covered during the "Foundations" course given to new employees at UWMC. GSA is covered during New Staff Orientation given at HMC.

3. Use of e-mail for work-related communications

Q: What is the standard for communicating UW Medicine information?
A: UW Medicine workforce members, including trainees, are required to use University of Washington (u.washington.edu), UW Medicine (uwp.org, uwp.washington.edu), or affiliates (cumg.washington.edu, seattlecca.org, fhcrc.org, psbc.org, med.va.gov, seattlechildrens.org) e-mail address and services when communicating UW Medicine information.

Q: What are the requirements for e-mail communications containing PHI within UW Medicine or communications between a provider and a patient?
A: These practices must be followed for all e-mail communications:

- Do not place PHI in the subject line.
- Only include the minimum necessary of PHI in the e-mail message.
- If you send or receive PHI, you are responsible for the protection and proper disposal of the information transmitted or stored in e-mail.
- Double-check the addresses of all recipients before sending confidential e-mail.
- Printed e-mail messages containing PHI must be disposed of properly, including shredding or secure recycling.
- The following e-mail "signature" or "footer" message must be included:

  The above email may contain patient identifiable or confidential information. Because email is not secure, please be aware of associated risks of email transmission. If you are a patient, communicating to a UW Medicine Provider via email implies your agreement to email communication; see http://uwmedicine.washington.edu/Global/Compliance/Pages/Risks-of-Using-Email.aspx

  The information is intended for the individual named above. If you are not the intended recipient, any disclosure, copying, distribution or use of the contents of this information is prohibited. Please notify the sender by reply email, and then destroy all copies of the message and any attachments. See our Notice of Privacy Practices at http://uwmedicine.washington.edu/Global/Compliance/Pages/Notice-Of-Privacy-Practices.aspx.

- E-mailing PHI outside of UW Medicine is not allowed unless end-to-end encryption using technologies such as TLS, S/MIME and PGP/GPG are used or the attachments are encrypted. UW Medicine strongly discourages e-mailing confidential information in this fashion at all.

Q: Can I automatically forward my UW e-mail account to a non-UW e-mail account (i.e., personal e-mail accounts such as AOL, Comcast, Hotmail, Yahoo, etc.)?

A: No. You are not permitted to set your UW e-mail account to automatically forward to a personal e-mail account. However, you may forward your email account to the following domains: cumg.washington.edu, seattlecca.org, fhcrc.org, psbc.org, med.va.gov, and seattlechildrens.org. (For the latest list of acceptable automatic forwarding domains please see UW Medicine Information Security SEC-03.02 Email Standard Policy at http://security.uwmedicine.org/Policies/SEC03.02-Email_Standard.htm.)