

Protecting Patient Information Self-Study

In this training, you will learn to identify when you can access and share patient information, understand how you can protect patient information at UW Medicine and recognize individual rights protected under HIPAA and know what to do when a patient raises them.

Patient Privacy

Every UW Medicine workforce member is personally and professionally responsible for the privacy, security and integrity of Protected Health Information (PHI) in any format (electronic, paper or verbal) entrusted to you. Your personal, professional and ethical responsibility is to protect all information used in your work for UW Medicine.

What is PHI?

PHI includes any information (verbal, paper or electronic) maintained or transmitted by UW Medicine that relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual, or payment related to the provision of healthcare.

Accessing and Sharing PHI

PHI may only be accessed or shared when it relates to your assigned job responsibilities, such as providing treatment to patients, how we bill and receive payment for patient care, or the operations of the health system. Access must be permitted by state or federal law and based upon a patient’s signed authorization.

Breaches

A breach is the acquisition, access, use or disclosure of PHI or PII for non-authorized reasons. Consequences of a breach are significant and damaging not only to UW Medicine but to patients, employees and contractors:

Reputation

- Loss of trust in organization and its workforce members

Investigations

- Subject to an investigation reported to your department, leaders, external agencies and patients

Resources

- Time and resources spent responding to an investigation, retraining, cost of legal counsel

Liability

- Potential for disciplinary actions, up to and including termination. Imposition of civil/criminal penalties, fines and sanctions.

Breach Examples

- Lost or stolen device containing unencrypted PHI
- Accessing the PHI of others “out of curiosity”
- PHI sent to the wrong location via email, fax, or mail
- Paper PHI not disposed of properly or given to the wrong person
- PHI compromised by phishing or malware

It is your responsibility to protect patient privacy: To protect PHI in all forms (verbal, paper, electronic), think about:

- **Where you are** – do not leave PHI unattended
- **Who might overhear** –be aware of your surroundings, volume and tone

- **Who might see** – physically secure PHI paper in lockable cabinets, lock your workstation or log out of your computer session when not in use, do not leave PHI on copy machines, fax machines or printers, ensure PHI is disposed of properly in shred bins
- **Am I sharing more than necessary** – except for treatment, we must limit accessing or sharing of PHI to the minimum amount needed to accomplish the intended purpose

Information Security and Data Stewardship

Take the proper steps to secure and protect all confidential UW Medicine information:

- Encrypt and password protect data on all mobile devices used for work purposes
- Save patient information to your department's shared network drive
- Use approved cloud storage solutions (not Dropbox or iCloud)
- Do not use email to send confidential information unless it is encrypted or sent through an approved email domain
- Do not input PHI into unapproved locations (e.g., free personal software programs, websites, or AI models).
- Obtain approval to take PHI offsite and do not leave it unattended
- Use antivirus software
- Always store information in secure places and secure portable devices such as laptops
- Use remote access (e.g., SSL or VPN) when working off-site
- Use secure logins (Do not use anyone else's username and password and do not share your username and password with anyone else, change your password at least every 120 days and choose passwords that are easy to remember, but hard to guess.)
- Lock your workstation or log out of your computer session when not in use
- **Report all possible breaches to the IT Help Desk (uwmhelp@uw.edu) or your supervisor**
- **If you clicked on a phishing link and submitted your username and password, report the compromise to UW-IT at help@uw.edu and the ITS Help Desk at uwmhelp@uw.edu.**

Malware, Ransomware, and Phishing

Malware mimics legitimate activity to perform harmful actions on your computing device. Ransomware is a type of malware that encrypts your files and prevents you from accessing them unless you or your organization pay a ransom. Phishing is an attempt to 'trick' you into providing your password or other credentials.

- Do not click on unknown links or pop-up windows
- Do not open an email or attachment from an unknown source
- Permanently delete suspicious emails from your inbox and deleted items

Electronic PHI (ePHI) Disposal

- Remove data prior to disposal, recycling or reassignment of electronic devices
- Empty your electronic trash bin regularly
- Contact your entity IT Department for help

Social Media

Social media includes websites and applications that enable users to create and share content or participate in networking. Examples: Blogs, bulletin boards, social networking sites, news media sites, photo and video sharing sites. The use of social media is prohibited when use would compromise patient confidentiality, and in unit work areas, unless social media use in these areas has been previously approved by a supervisor. PHI or any combination of patient information/pictures that could reasonably identify a UW Medicine patient may not be posted on social media.

Patient Rights Under HIPAA

Patients have the right to access, inspect, copy and request amendments to their PHI. Patients also have the right to request alternative forms of communication and restrict uses and disclosures of their PHI. If you receive these requests, direct the patient to contact your entity Release of Information department for help.

Patients may request an accounting of disclosures (a report of instances when a patient's PHI was disclosed outside of Treatment Payment or Operations (TPO)), authorized releases, and limited data set uses. Contact UW Medicine Compliance with an accounting of disclosures request.

Compliance Services

UW Medicine Compliance is here to help when you have questions or concerns. You may contact us via phone, 206.543.3098, email (comply@uw.edu) or through our anonymous hotline - 206.616.5248 (local) or 866.964.7744 (toll free).

RESOURCES:

Incident Reporting Resources

- If your computer or mobile device is infected, or you think it may be infected, contact IT Security immediately
- Report information security incidents when they occur. Contact IT Services Help Desk at uwmhelp@uw.edu. If it is urgent, call 206-520-2200.
- Report the loss or theft of PHI to UW Medicine Compliance at 206-543-3098 or comply@uw.edu immediately

IT Security Resources

- [UW Medicine Information Security Program](#)
 - [Identity and Access Management Standard](#)
 - [Approved Email Domains](#)

Compliance Resources

- [UW Medicine Compliance Website](#)
- [UW Medicine Compliance Social Media Policy & Guidance](#)
- [UW Medicine Compliance Code of Conduct](#)
- [UW Medicine Compliance Privacy FAQs](#)

UW Medicine Compliance Department

206.543.3098, Email: comply@uw.edu

ATTESTATION:

Date: _____

I, _____, certify that I have read and understand the Protecting Patient Information Self-study.

Signature: _____

Print Name _____

Name of Manager: _____

Department: _____

After signing this form, please give it to your supervisor. Signed forms are kept in your personnel file.