Protecting Patient Information Training
Self-Study

Through this training you will learn to how to identify and protect patients' protected health information, gain access to helpful resources and assist UW Medicine in ensuring our patient's rights and reducing organizational risk.

UW Medicine

COMPLIANCE

UW MEDICINE COMPLIANCE		
206.543.3098	1.855.211.6193	comply@uw.edu
Anonymous Hotline	206.616.5248	1.866.964.7744

What is Protected Health Information?

We are required by law to protect our patients' Protected Health Information or **PHI.** PHI is verbal, written or electronic information relating to a patient's past, present, or future physical or mental health including care or condition. Our obligation to protect PHI remains even if the patient is deceased.

You must remove all 18 identifiers to de-identify PHI.

PHI	
1. Names	10. Account Numbers
2. Geographic Identifiers	11. Certificate or License Numbers
3. Dates	12. Vehicle Identifiers, Including License Plates
4. Phone Numbers	13. Device Identifiers and Serial Numbers
5. Fax Numbers	14. URLs
6. Email Addresses	15. IP Addresses
7. Social Security Numbers	16. Biometric Identifiers
8. Medical Record Numbers	17. Face Photographic Images
9. Health Plan Beneficiary Numbers	18. Any Other Unique Identifier

Treatment, Payment, Healthcare Operations

PHI may be used, or disclosed for:

- **Treatment**: the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another.
- **Payment**: all activities undertaken by UW Medicine to obtain reimbursement for treatment provided.
- **Healthcare Operations**: certain administrative, financial, legal, and quality improvement activities of a covered entity necessary to run its business and to support the core functions of treatment and payment.

When disclosing PHI:

- Except for treatment purposes: use the **MINIMUM** amount of PHI necessary to accomplish the intended purpose.

Authorizations

An authorization is a written document that gives permission to use and disclose PHI.

- Authorizations are required for uses and disclosures not otherwise permitted or required by law.
    - May be required for release of PHI for:
        - Employment
        - Photography
        - Media Use
- A valid authorization must be written in plain language and contain required elements.

Contact your entity's Health Information Management department for the appropriate form.

Breaches of PHI

Follow all UW Medicine privacy policies and procedures to help avoid a breach of our patients' PHI. A breach is the acquisition, access, use or disclosure of PHI that is:

- Not for treatment, payment or healthcare operations
- Not authorized by the patient
- Not otherwise allowed by law; and
- Compromises the security or privacy of the PHI

Breach examples may include:

- PHI sent to the wrong location via fax, mail, etc.
- Unencrypted, lost or stolen devices containing PHI
- Improper disposal of documents containing PHI
- Accessing or sharing PHI outside of job duties
- PHI handed to the wrong patient or person

Consequences of a breach are both institutional and personal and include:

- Loss of Trust
- Reputational Damage
- Investigations
- Fines, Sanctions and Imprisonment
- Re-Training
- Loss of Privacy for the Patient

When a breach occurs, UW Medicine may be required to notify the:

- Individual Patient
- US Department of Health & Human Services Office for Civil Rights

UW Medicine is obligated to notify patients of a breach of their PHI.

If you suspect a breach, notify UW Medicine Compliance.

Research: Patient Authorizations or Waiver Requests

PHI may be used or disclosed for research purposes when UW Medicine agrees to the disclosure and when one of the four following conditions is met:

- Approval from the IRB* with authorization of the patient
- Permission from the IRB* to use and disclose a subject's PHI without obtaining their authorization (Waiver of Authorization)
- The PHI has been de-identified by an approved method
- When the PHI is part of a limited data set and an authorization for use and disclosure of the data is in place (Data Use Agreement)

UW Medicine will disclose only the minimum amount of PHI necessary to accomplish the purpose of a given request for the use and disclosure of patient information for research.

Limited Data Set is PHI where these 16 identifiers must be removed from the patient's health information.	
1. Names	9. Account Numbers
2. Postal address information other than town or city, state, and zip code	10. Certificate or License Numbers
3. Telephone Numbers	11. Vehicle Identifiers, Including License Plates
4. Fax Numbers	12. Device Identifiers and Serial Numbers
5. Electronic mail addresses	13. URLs
6. Social Security Numbers	14. IP Addresses
7. Medical Record Numbers	15. Biometric Identifiers (including finger and voice prints)
8. Health Plan Beneficiary Numbers	16. Full Face Photographic Images and any comparable images

The Institutional Review Board (IRB) is a committee established to protect the rights and welfare of human subjects by reviewing and approving applications for research projects.

Compliance is EVERYONE's Responsibility

Your Role:
Responsible for understanding and adhering to relevant policies and procedures, participating in required training, fulfilling recordkeeping requirements, reporting compliance concerns, seeking clarification when questions arise, and responding in a timely manner to requests for information associated with internal audits or investigations.

Supervisor Role:
Responsible to communicate compliance and operational expectations, ensure that appropriate training is taken, implement and enforce policies, and monitor compliance.

Senior Leadership Role:
Responsible for participating in the development and implementation of UW Medicine-wide systems. They are entity champions supporting successful implementation and sustenance of compliance and related operational programs within their specific areas of oversight.

Compliance Role:
Monitor developments in the regulatory environment, establish entity-specific policies and standards, work closely with operational departments to develop internal controls, receive and investigate allegations of noncompliance, develop and implement effective auditing programs, and provide compliance training.

UW Medicine Board Compliance Committee Role:
Advisory responsibilities including strategic planning, advocacy and support for compliance efforts, risk assessment and analysis of compliance issues. Additional committees within UW Medicine provide mechanisms for engaging administrative, clinical and operational leaders in compliance initiatives.

If you see something that doesn't look right or could be a potential compliance problem, contact UW Medicine Compliance.

Responsibility for Safeguarding PHI

Requirement: Safeguard PHI in all of its forms. This means you must use reasonable methods to prevent improper uses and disclosures of PHI.

In order to protect PHI in all forms (verbal, paper, electronic), think about:

- Where you are
- Who might overhear
- Who might see
- Your patients' privacy

Avoid:

- Discussing PHI in front of others who do not need to know
- Leaving PHI unattended, or otherwise accessible to patients and others who do need to see it
- Positioning monitors where others can view them
- Printing to devices located in public or unsecured areas

For storage and disposal of documents with PHI, think about the following:

- Keeping track of documents containing PHI
- Disposing of PHI in Shred-It containers and not in trash or recycle bins
- Securing documents when they are not in use
- Deleting all electronic PHI when no longer required for your job
- Locking cabinets when not in use

Good computer and electronic document practices are key to safeguarding PHI.

- Use a secure network server
- If this is not possible, do not save files containing PHI to desktop computers unless both the computer and the files are encrypted
- Use a privacy screen on your computer monitor
- Lock (CTRL-ALT-DELETE) your workstation or log out of your computer session when not in use

Transporting Confidential Information Safely

Keep paper and devices containing PHI with you at all times (note that mobile devices must be encrypted).

- Place paper documents containing PHI behind a locked barrier when not in use
    - Lock your office when you are away from it
    - Lock your cubicle overhead bins, filing cabinets, etc.

Do not leave paper and devices locked in your car.

Passwords

Your password provides a line of defense against unauthorized access. The stronger your password, the greater protection it offers.

- Change passwords often – at least every 120 days
- Do not store passwords on sticky notes, an Outlook Calendar, or other unprotected means such as Word or Excel

Examples of Complex Passwords
At least 8 characters long
Contain at least 1 symbol
Contain at least 1 numeric character
A mix of upper and lowercase letters

Best practice is to use a password manager program.

- A password manager is a software application that stores and organizes passwords. Passwords are usually encrypted, requiring the user to create a master password (a very strong password that grants you access to your entire password database).

Mobile Devices

Mobile devices pose a risk to PHI.

Mobile Devices Include
Smart Phones
Laptops and Tablets
Thumb, jump, or USB drives
External Hard Drives
Any other small computing device that has a display screen with touch input and/or a miniature keyboard

If you use a mobile device for work, it contains PHI. Mobile devices **must be encrypted**.

- Never assume mobile devices are encrypted out-of-the-box.
- Encryption protects the data storage units inside devices and renders them unreadable..
- Encryption is not the same as password protection. **You need both**.

Password protection AND encryption greatly reduce the likelihood of a breach of PHI in the event of loss or theft.

- Follow the manufacturer instructions as well as your entity's specific process. Contact IT Support for assistance with device encryption. Follow mobile security guidelines for Android and iPhone. *
- Most mobile devices are enabled with 'find and wipe' applications that allow you to remove data if lost or stolen. Follow the manufacturer's guidance to enable.

For workforce members with UW NetID only: VMC workforce members, please contact IT Support at x6200 or ithelp@valleymed.org.

Remote Computing

For Remote Computing use:

- Remote access programs (e.g., SSL VPN, extranet) when working offsite. This keeps information on secure networks and off your mobile or remote device.
- Web-based email tool to access your email when working remotely. This keeps your email on the server, not on your device. Configure your email (Outlook) to not cache locally.
    - Cache is the storage of data that makes future requests for the same data more efficient.

Contact IT Support for guidance.

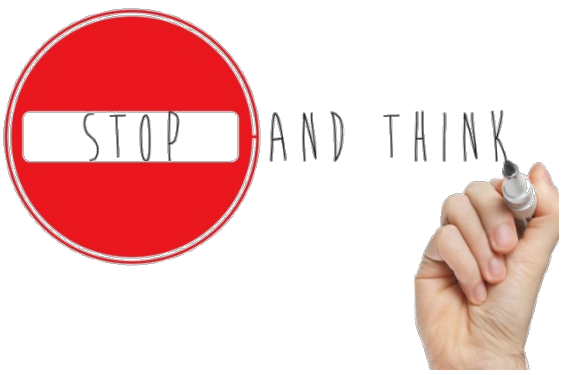
Protect Yourself Against Malicious Software and Phishing: General Advice

Malicious software mimics legitimate activity in order to perform harmful actions on your computing device.

- UW Medicine is a data rich environment. As a result, we are a target for actions by those trying to maliciously access our data
- If you receive a call from someone alleging to be IT, hang up and call IT to determine legitimacy

Phishing is password harvesting and is an attempt to 'trick' you into providing your password or other credentials.

- Clicking on links in email or on the web puts PHI at risk of inappropriate access or corruption
- Never provide your password, no one within UW Medicine will ever ask for it



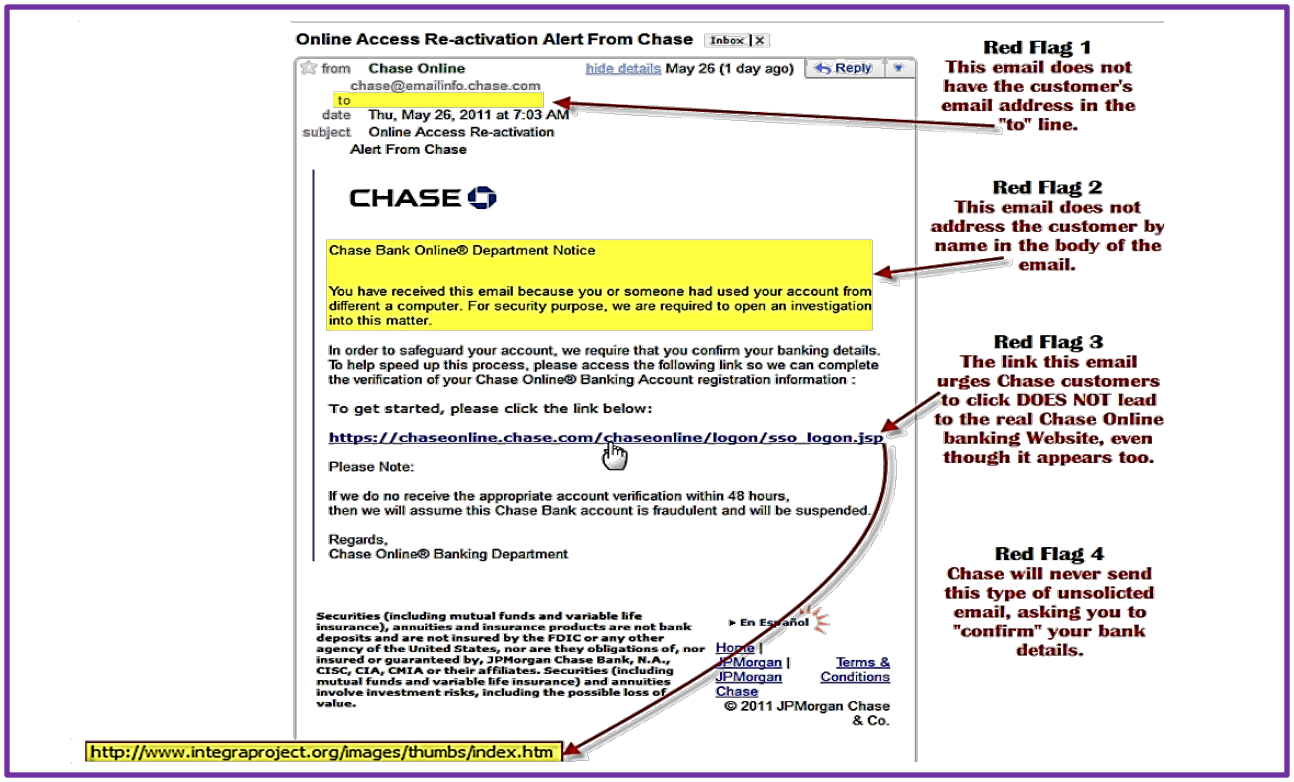
Protect Yourself Against Malicious Software and Phishing: Email

- Assume unexpected and unknown email is an attack
- Only open email and attachments from known sources
- Verify unexpected links and attachments with sender and/or IT Support
- Forward suspicious email to uwmed-abuse@uw.edu
- Fully delete email from inbox and sent-mail
- Report warning message from your antivirus software to IT Support

Email containing PHI must be encrypted.

Contact IT Support for assistance with the following:

- Sending an email outside of the approved domain list
- Instructions on how to send an encrypted email



Protect Yourself Against Malicious Software and Phishing: Web

- Avoid using work computer for personal use
- Avoid web pages with misspellings in the web addresses and site names
- Roll cursor over website links to see where they are actually going
- Be wary of websites that promote schemes involving recruiting others or receiving or giving money
- Comply with browser alert messages when they detect an unsafe site

Do not click on unknown links or pop-up windows

Disposal of Electronic PHI and Devices Containing PHI

- Remove data prior to disposal, recycling, or reassignment of electronic devices (e.g., fax machine, biomedical device, desktop computer, or mobile device)
- Empty your electronic trash bin regularly
- Deleted files and emails may still exist on your device until you empty the trash bin

Contact IT Support for assistance with above practices.

Social Media

Social media includes websites and applications that enable users to create and share content or participate in networking.

Online examples:

- Blogs
- Bulletin boards
- Social networking sites
- News media sites
- Photo and video sharing sites

UW Medicine policy prohibits the use of social media in clinical settings. PHI does not belong on blogs or social sites under any circumstances.

HOW TO OBTAIN ASSISTANCE:

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 mcsos@u.washington.edu. If it is urgent, call 206-543-7012
- 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: https://depts.washington.edu/uwmedsec/
- Northwest Hospital ITS: http://nwh/sites/operations/ims/SitePages/Home.aspx
- Valley Medical Center ITS: https://valleymed.sharepoint.com/sites/policycentral/PolicyCentral/Forms/IT/aspx

Permitted Uses and Disclosures

You may use or disclose PHI without authorization in the following situations:

- With the patient
- For Treatment, Payment and Healthcare Operations (TPO)

With the exception of TPO, you must account for all disclosures made without patient authorization.

Contact Compliance to learn how to make an accounting of disclosure entry.

Use is the sharing application, utilization, examination or analysis of PHI within UW Medicine.

Disclose is the release, transfer, access to, or sharing of PHI outside UW Medicine.

For **Public Policy Purposes** include disclosures:

A. As required by law

B. About victims of abuse, neglect or domestic violence

C. For health oversight activities

D. For judicial and administrative proceedings

E. For research

F. To avert a serious threat to health and safety

G. For workers' compensation

When a Patient Has the Opportunity to Agree or Disagree

A patient must be given the opportunity to agree or disagree to the following uses and disclosures:

- Exclusion from the Facility Directory
- Providing proof of immunization to schools
- Interaction with law enforcement (photography and evidence gathering)
    - Except when in custody
- Sharing PHI with family, friends and other designated individuals involved in their care
    - Unless the patient objects:
        - You may disclose their PHI to relatives or other people involved in the patient's care or payment related to patient's healthcare.
        - If a patient is unable to agree or disagree, you may disclose, if based on your professional judgement, it is in the best interest of the patient.

Requires a Signed Patient Authorization

A valid authorization is required for use and disclosure of PHI except for the purposes of treatment, payment and healthcare operations or when allowed or required by law.

Do not disclose PHI of heightened confidentiality unless written authorization explicitly allows it, examples may include:

- Records relating to testing or treatment for STD testing or treatment and reproductive health
- Behavioral or mental health treatment records
- Substance abuse treatment records

Notice of Privacy Practices

UW Medicine must provide patients with the Notice of Privacy Practices (NoPP) that explains:

- How UW Medicine protects patients' privacy and how it will use and disclose their PHI
- How patients can get assistance and information about their privacy rights
- How patients can file a privacy complaint
- How to contact UW Medicine Compliance

Check with your supervisor if your role requires you to provide the NoPP to patients.

Access, Inspect, and Copy PHI

With few exceptions, patients have the right to:

- Access
- Inspect
- Receive a copy of their own PHI

If you receive a request, direct the patient to contact your entity's HIM Department for assistance.

Amendments to PHI

Patients have the right to request an amendment to their PHI.

- Entity HIM departments facilitate PHI amendments
- UW Medicine must respond to the requests within 10 days upon receipt

UW Medicine may deny the request when the:

- Healthcare provider determines the PHI is accurate and complete; or
- PHI was not created by UW Medicine

Patients have the right to disagree with UW Medicine's denial and may submit a written disagreement letter to the HIM Department.

UW Medicine may rebut the patient's disagreement letter in writing.

When releasing the patient's records, UW Medicine must include all documents created in response to the Patient's initial amendment request.

Alternative or Confidential Communications

Patients have the right to request:

- Verbal versus written communications
- Written versus verbal communications
- Electronic versus paper
- Fax versus postal mail
- Postal mail directed to an alternate address
- Phone calls directed to an alternate phone number

This is called the patient's right to alternative or confidential communication.

HIM departments will determine if UW Medicine is able to comply with confidential communication requests and communicate with the patient.

Disclosure Restrictions

Patients have the right to request restrictions on uses and disclosures of their PHI.

For example, patients may request that UW Medicine does not:

- Share their PHI with previous providers or certain family members
- Bill their insurance when the patient selects to pay for the services received out of pocket

Direct patient requests for restrictions to your HIM department.

Accounting of Disclosures

Patients have the right to receive a report of instances when their PHI was disclosed outside of:

- Treatment, Payment, or Operations (TPO)
- Authorized releases
- Limited Data Set uses

This is called an Accounting of Disclosures.

Contact UW Medicine Compliance with an accounting of disclosures request.

Make a Privacy Complaint

Patients have the right to file a complaint regarding the privacy of their PHI through:

- Mail
- Phone
- Fax
- Email.

Contact UW Medicine Compliance with patient complaint questions.

UW MEDICINE COMPLIANCE		
206.543.3098	1.855.211.6193	comply@uw.edu
Anonymous Hotline	206.616.5248	1.866.964.7744

UW Medicine
Protecting Patient Information Self Study
Signature Page

UW Medicine
COMPLIANCE

Date: _____

I, _____certify that I have completed the Protecting Patient Information Self Study on the confidentiality of patient health information (PHI), specifically the privacy regulations adopted pursuant to federal Privacy and Information Security regulations (45 CFR Parts 160 and 164 (HIPAA)).

I understand that I must maintain the confidentiality of individual healthcare information and agree to comply with UW Medicine Compliance policies and procedures located at http://depts.washington.edu/comply/patient_privacy/.

Signature: _____

Print Name: _____

Name of Manager: _____

Department: _____

Please complete this form and provide the original to your manager. Send a copy to UW Medicine Compliance (mail to: Box 358049, email to: comply@uw.edu, or fax to: 206.221.5172) to receive credit for completing your required HIPAA training.

Manager: Documentation to be maintained in workforce member department record and by UW Medicine Compliance.

File original in departmental personnel file.