Note

- **The following HIPAA training is intended for Vendors, Business Associates, Students, Pre-Approved Shadowers, and Visitors.**
- **The following training module does not provide credit for annual training for employees.**
- **Use your down arrow key to begin the training.**

Note: If you are an employee, employees must login and take the HIPAA training through the approved Learning Management System at *https://hrit.utah.edu/lms/#/*

Welcome to the University of Utah Health

HIPAA Privacy and Security Training Program

Vendors, Business Associates (BAs), Pre-Approved Shadowers, Students, Volunteers, and Visitors

"You cannot have Privacy without Security."

HEALTH
UNIVERSITY OF UTAH

Vendors, BAs, Students & Shadowers

Vendors, Business Associates (BAs), Students, and Shadowers, (also Volunteers and Visitors [who are not patients and/or not accompanying or visiting patients]), coming into the UUH facilities must:

- Sign a UUH Visitor's Confidentiality and Security Agreement
- Complete the required UUH HIPAA Privacy and Security training
- Obtain and be identified with a name tag or controlled UUH ID badge
- Understand and follow UUH policies and procedures

Requirements

Individuals "shadowing" health care professionals or observing patient care in UUH must also have:

- A sponsor
- A complete and approved shadowing form
- Permission from the sponsor's direct supervisor
- Consent from the patient*

*Patient consent may be verbal or written but **must** be documented.

Information Security and Privacy Commitment

- ✓ **Protect the *privacy* of each patient, student, employee and client;**
- ✓ **Guard the *confidentiality* of all UUH patient information;**
- ✓ **Keep the *integrity* and honesty of all recorded information; and**
- ✓ **Ensure reasonable *security and availability* of all electronic information.**

Protected Health Information

PHI

Definition of PHI

Protected Health Information (PHI) includes:

- **Any** health information created, received, sent, or kept by University of Utah Health (**UUH**).
- Any information, **in any form**, that is related to the past, present, or future physical or mental health or condition of an individual; or payment for services.
- Health and demographic information that can be used to identify an individual.

PHI Comes in All Forms…

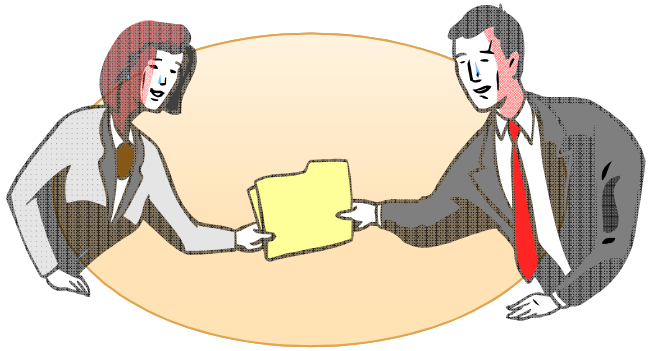
- **Spoken / Verbal Communications**
- **Paper or "Hard Copy"**
  - Forms
  - Documents
  - Paper charts
  - Labels on patient care items
  - Photos, X-rays and graphics

- **Electronic**
  - Electronic Medical Records - EMRs (i.e., EPIC, PowerChart)
  - Computer spreadsheets, lists, notes, etc.
  - Video, audio recordings
  - CDs, DVDs, tapes
  - Etc., etc., etc. …

…PHI must be protected!

The “Minimum Necessary” Rule

- **Limit the uses, disclosures and requests for Protected Health Information (PHI) to the “minimum necessary” to do your job**
- **Be sure to get the required documentation when using, disclosing or requesting PHI**



How We Use and Disclose PHI

Treatment, Payment
and Healthcare Operations
TPO

HEALTH
UNIVERSITY OF UTAH

Treatment, Payment & Operations

We may use and share patient health information (PHI) as we do our jobs

T
P
O

- **Treat Our Patients –**
  - **We can use health information and share it with other professionals who are *treating* or are *directly involved* in the patient's care**
- **Bill and Receive Payment**
  - **Health information may be used and shared to *bill and get payment* from health plans or other entities**
- **Improve Our Organization**
  - **We can use and share patient's health information to *run our organization and improve care***

How We Use and Disclose PHI

Special Situations*

*Authorized personnel only

HEALTH
UNIVERSITY OF UTAH

Special Situations*

We may share patient information in ways that contribute to the public good

- **To help with public health and safety issues**
- **To do approved research**
- **To respond to organ and tissue donation requests**
- **If state or federal law require it**
- **To work with a medical examiner or funeral director when an individual dies**

*Authorized personnel only

Special Situations* (cont.)

- **For worker's compensation claims**
- **For law enforcement purposes (must be authorized in writing)**
- **For law, military, national security reasons and/or presidential protective services**

  - **Note: In response to law enforcement, legal actions and lawsuits, w**e will ***only*** share health information in response to a court order or subpoena signed by a judge

*Authorized personnel only

How We Use and Disclose PHI

Research

HEALTH
UNIVERSITY OF UTAH

Research

Research

- UUH may use or disclose *de-identified* patient information for authorized research purposes
- **Institutional Review Board (IRB)** approval is required including:
  - Documentation, IRB number, IRB review, approval, and appropriate signatures
- The use of *de-identified* information for research is not subject to HIPAA
  - **De-identified patient information has to meet a special de-identification process**

Contact the department study coordinator or the Institutional Review Board (IRB) with questions

How We Use and Disclose PHI

PHI for Patient Care

HEALTH
UNIVERSITY OF UTAH

Sharing PHI with a Patient's Family

When family and or friends accompany a patient to UUH…health information may be shared:

- **If** we **ASK** the patient and they give their oral consent;
- **If** the **patient does not actively object**;
- **If** the family and/or friend are going to be **involved in the patient's care outside of UUH**, only give the **amount of information necessary to care for the patient**.

Patient Rights

Patient Rights

- **Patients have the right to:**
  - Access and request a copy of their records
  - Amend their records
  - Designate a personal representative
  - Receive a copy of the UUH Privacy Notice
  - Request an accounting of disclosures
  - Request confidential communications
  - Request that we do not bill their insurance
  - Request special privacy restrictions

Patient Rights

- Patients may request their records in paper or electronic format
- Send patients/individuals with requests regarding their medical records to Health Information (Medical Records) at 801-581-2704

Your Access to PHI

Access to Other's PHI

It is A VIOLATION OF UNIVERSITY POLICIES to open or look at the protected health information (PHI) of ANY PERSON including children, family members, co-workers, friends, supervisors, high profile patients, etc., unless you are part of the care team.

You may **NOT** access the records (PHI) of your family members using the electronic medical record system(s) (EMRs), even with written authorization. You must go to the Health Information Department to request access for family members' health records.

Questions regarding release of PHI?
Contact **Health Information** (Medical Records) 801-581-2704

UUH Encryption Processes

Encryption Process

ALL laptops, USB drives and external storage devices that are used to conduct University of Utah Health business MUST be whole disk encrypted. (Call the Hospital Help Desk at 801-587-6000 with questions.)

- This applies to **ALL** devices *(used to conduct UUH business)* regardless of whether they are personally owned or issued by the University.
- If USB devices are not encrypted, access to the network will be denied.

Approved encrypted USB drives are available at the University Bookstore and can also be ordered by authorized individuals through Asset Management at http://UUH.utah.edu/asset/

Email and PHI

- **If you must send restricted or sensitive information through email:**
  - Limit the amount of sensitive information to **"need to know"** to get the task done
  - Send to single addressee only, not to distribution lists or list serves, and **double check the address**
  - **Encryption** resources are available **only** through the University of Utah email system **(Umail)**
  - Use only your **Umail** email account for any work-related efforts (…@...utah.edu)

Email and PHI

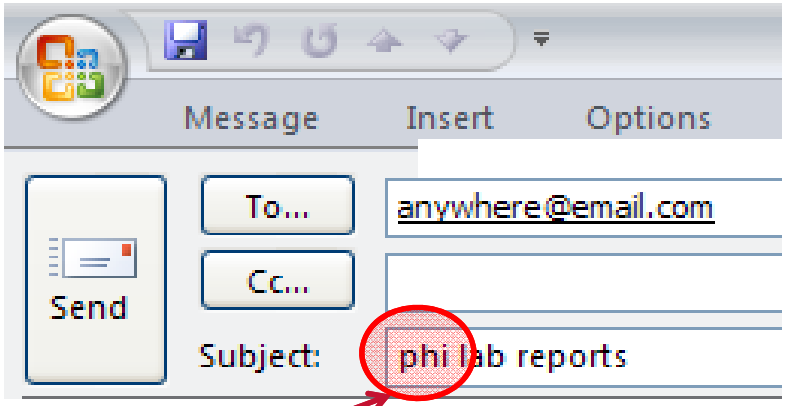
- ***Do not send PHI using a non-University personal email account* (i.e., MSN, Hotmail, Yahoo, Gmail, etc.):**

  - Sending PHI using a non-University personal email is a violation of University policy
  - Risks the privacy of our patients' health information
  - Puts the University at financial and reputational risk
  - May subject you to disciplinary action
- ***Do not Auto-Forward* email (including PHI) *to your personal email account* (i.e., MSN, Hotmail, Yahoo, Gmail, etc.):**
  - Others have no way of knowing you are auto-forwarding
  - Email could be auto-forwarded without being encrypted
  - Puts our patient's PHI, you and our organization at great risk

How to Encrypt Email…

To encrypt a message from your issued Umail account, simply add the letters **PHI** to the *subject line* of the message

- ✓ Both uppercase or lowercase **PHI** / **phi** are effective.
- ✓ **Do not include any personal identifiable information in the subject line**.
  - ➢ **Note**: The **subject line** of the email is not encrypted.



- ✓ **The code PHI must stand alone…**words containing phi, i.e., philosophy, or punctuation next to phi…i.e., phi:, phi,, phi-, phi=, etc., will not activate the encryption program.

Prevent and Report PHI Data Disclosures

HEALTH
UNIVERSITY OF UTAH

Prevent Unauthorized Disclosures…

- Think before you act!
- *Be careful* when sending PHI
- Verify correct recipient is getting correct info
- Limit information to "need to know"
- Encrypt email; remember to use 'PHI' in the subject line
- Verify fax numbers and always dial full 10 digit fax numbers (area code + number) even within UUH
- Lock and/or log off your computer when unattended
- Never share passwords
- Never, ever share accounts
- Encrypt all laptops and USB drives
- Do not store PHI on laptops or portable media
- Backup your files to the network drive
- At end of life, dispose of PHI by shredding or destroying

You Will Be Protected

Anyone who makes a report to the Privacy Office as required by HIPAA will be protected. It is a violation of University of Utah policy and federal law to intimidate, threaten, or harass anyone who exercises their rights and *responsibilities* under HIPAA by filing a complaint or reporting a privacy and/or security issue.

***It's the Law*.**

Business Associates
and
Business Associate Agreements

Business Associates

- A ***Business Associate*** is a person or company who does something for UUH or on our behalf and with whom we share PHI.
- A ***Business Associate Agreement*** outlines permitted use, disclosure, restrictions, and outlines any safeguards to protect any restricted information that may be shared with the business associate.
  - Questions regarding Business Associates or a Business Associate Agreement should be directed to the Privacy Office at 801-587-9241

Business Associate Agreements

- **A *Business Associate Agreement* (BAA) spells out:**
  - How the Business Associate will use/disclose our PHI
  - Appropriate safeguards to protect our information
  - That the Business Associate will develop a BAA with all their sub-contractors
  - That the Business Associate will have our PHI available on request and available for amendment and/or available for accounting of disclosures
  - At termination of the contract, all PHI must be returned or destroyed or the PHI contract protections may be extended

Questions about Business Associates should be referred to the Information Security and Privacy Office at 587-9241.

Violations and Sanctions

(Sanctions = Consequences)

HEALTH
UNIVERSITY OF UTAH

University of Utah and UUH penalties apply, up to and including termination of the contract of the business relationship, if there is a **willful disregard** to policy.

Violating the Privacy and/or Security Rules can result in **personal liability,** civil or criminal sanctions, including fines, and/or jail-time.

Violations Include…

Improper use of **Passwords and/or sharing account information**. *Examples* may include but are not limited to:

– ***Allowing a co-worker to use your login,*** or using a co-worker's login, ***for any reason***

– ***Failure to report unauthorized use*** of an account or password belonging to someone else

*If **anyone** (even someone in a management position) asks you to share your account , **for any reason**, contact the Information Security and Privacy Office at www.privacy.utah.edu > "Report an Incident". Your report will remain confidential.*

Violations Include…

– **Getting into information** outside the "minimum necessary to do your job," and/or, outside your "professional need to know"…

- (i.e., for **personal reasons**, out of **curiosity** [co-workers, celebrities, high-profile patients, family, etc.], and/or at the **request of someone** who cannot, or does not want to log on under their own account, etc.)

– **Posting PHI or other personally identifiable data on the Internet (i.e., social networking sites)**

– **Installing or downloading unauthorized software** (i.e., Illegal Peer-to-Peer file sharing/distributing of movies, music, other media, copyright infringement, gaming programs, gambling, etc.)

Violations Include…

- Attempting to **avoid, or bypass the security mechanisms** of any IT resources
- **Illegally altering, destroying, or intentionally removing PHI** or other private data from the U of U/UUH
- **Selling** health or personal information; or inappropriately selling/giving such information to the news media
- **Transporting, taking home, or photocopying** of protected health information

Consequences Can Include…

U of U and UUH sanctions for violations can include:

- Loss of access to all computers and computer programs

Federal sanctions can include *personal liability* for…

- Civil Charges of between $100 to $1,000 each per standard / per violation / per year, up to $1,500,000, OR
- Criminal Charges up to $1,500,000 and 10 years in prison

HIPAA Enforcement

- **U.S. Dept. of Health and Human Services (HHS) will conduct periodic audits of University of Utah Health (*and our Business Associates*) to assess compliance**
- **"Enhanced Enforcement," as listed in HIPAA, permits State Attorneys General to pursue civil actions**
- **Mandatory monetary penalties will be imposed for "*willful neglect*" of privacy and security**

Information Security

Information security is essential to help mitigate risk and protect our IT resources (computer, servers, and other electronic devices).

- Secure and protect your physical environment
- Create strong passwords and keep your computer accounts safe and secure
- Avoid computer security risks at work, home and on the road
- Understand violations and consequences

Report Unauthorized Disclosures

If you discover a potential disclosure, or if you become aware of someone not following information privacy and security policies…

Report!

- ***Complete an incident report at: www.privacy.utah.edu***
- Immediately **Call** the Hospital Help Desk at 801-587-6000
  - Privacy personnel will be notified and will begin an investigation

Congratulations!

You have completed the HIPAA Privacy and Security training module for Students, Vendors and Shadowers.

Continue to the next slide, print and *sign* the attestation certificate.

Questions?

Contact the Information Security and Privacy Office at 587-9241

INFORMATION SECURITY AND PRIVACY OFFICE
THE UNIVERSITY OF UTAH

UNIVERSITY OF UTAH HEALTH

HIPAA PRIVACY AND SECURITY TRAINING

I attest that I have successfully completed the assigned HIPAA course of study required by University of Utah Health for Vendors, Shadowers and Visiting Students and will comply with the HIPAA Privacy and Security Regulations and University of Utah Health Policies and Procedures.

Print Name _____ Date _____

Signature _____