Note

• The following HIPAA training is intended for Students, Vendors, Business Associates, Visitors and Pre-Approved Shadowers.

• The following training module is a “not-for-credit” course and will not be recorded.

• Employees must take the HIPAA training through the approved Learning Management System at https://hrit.utah.edu/lms/#/.

• Use your down arrow key to begin the training.
Welcome to the University of Utah Health
HIPAA Privacy
and
Security Training Program

“You cannot have Privacy without Security.”
Requirements of All UUH Workforce Members

ALL University of Utah Health (UUH) workforce members are required to:

- **Sign** the Confidentiality and Security Agreement at the time of employment
- **Complete** HIPAA Privacy Information Security Training
- **Understand** and **Follow** UUH policies and procedures

**Workforce**
Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (University of Utah Health) or business associate, is under the direct control of such covered entity or business associate, **whether or not they are paid** by the covered entity or business associate.

*HIPAA § 164.530*
Information Security and Privacy Commitment

- Protect the *privacy* of each patient, student, employee and client;
- Guard the *confidentiality* of all University Health Sciences and 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

HIPAA § 164.520
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.

– 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 Health Insurance Portability and Accountability Act (HIPAA) mandates protection for the privacy and security of protected health information (PHI)

• HIPAA also requires:
  – We tell our patients about how we use and disclose their PHI
  – We tell our patients about their rights to manage their own health information

This is done through the ‘Notice of Privacy Practices’
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:

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.

Patient authorization for use of health information is not needed as we treat and care for our patients.

Examples of medical treatment or services:
Consultation, update referring physician, care coordination, prescribing, scheduling labs and/or radiology, continuity of care, etc.

HIPAA § 164.506
We may use and share patient health information (PHI) as we:

Bill & Get Payment for Services -

Health information may be used and shared to bill and get payment from health plans or other entities.

Patient authorization for use of health information is not needed as we bill and get payment for services.

Examples include giving information to health insurance plans so they will pay for our services.
We may use and share patient health information (PHI) as we:

Run our Business Operations -

We can use and share patient’s health information to run our organization and improve care.

Patient authorization for use of health information is not needed as we run business operations.

Examples: Run our organization, business operations, training, develop more effective treatment, establish new/different service needs, cooperate with other providers/health plans to improve care, reduce costs, comply with Federal & State laws.
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 any necessary documentation when using, disclosing or requesting PHI for TPO.

HIPAA § 164.514
How We Use and Disclose PHI

Use and Disclosure for Special Situations
Special Situations

We may share patient information (without authorization) in ways that contribute to the public good

– To help with public health and safety issues
  • Preventing disease, help with product recalls, reporting adverse reactions to medications, reporting suspected abuse or domestic violence, preventing or reducing a threat to anyone’s health or safety

– Do research
  • We can use or share health information for health research
Special Situations (cont.)

– Respond to organ and tissue donation requests
  • We can share health information without authorization with organ locating and donation organizations

– Required by law
  • We will share health information if state or federal law require it, including with the Department of Health and Human Services (HHS) if there are requests to verify we are complying with the federal privacy law

– Work with a medical examiner or funeral director when an individual dies
Special Situations (cont.)

– Address workers’ compensation, law enforcement purposes or officials, and other governmental requests in writing
  • For worker’s compensation claims, for law enforcement purposes, must be authorized in writing by law, military, national security reason, and/or presidential protective services

– Respond to lawsuits and legal actions
  • We will share health information for lawsuits and legal actions only in response to a court order or subpoena signed by a judge
How We Use and Disclose PHI

Use and Disclosure for Research
Research

– UUH may use or disclose patient information for 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 information has to meet a special identification

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

HIPAA § 164.512; § 164.514
Definition of De-Identification for Research

Requires removal of **ALL** of the following identifiers of the individual *and* of relatives, employers, or household members from medical record information:

1. Names
2. All geographic subdivisions smaller than a State, including zip code except for the initial 3 digits;
3. All elements of dates (except for year) including birth date, admission date, discharge date, date of death
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code*

*except a code to permit re-identification of the de-identified data by the Honest Broker

HIPAA § 164.514
How We Use and Disclose PHI

Use and Disclosure of PHI of Decedents
Decedents

• NEW under HIPAA
  – HIPAA protects the PHI of a decedent for 50 years after death.
  – Person with testamentary authority or other relationship as personal representative can authorize disclosures
  – If individual is deceased more than 50 years, HIPAA protections no longer apply.

Requests for decedents records can be referred to Health Information (Medical Records) 801-581-2704
Accounting of Disclosures

Limit use and disclosure of PHI to the “minimum necessary” to do your job.

Be sure to provide the necessary documentation for special situation uses, disclosures and requests for PHI.

Use the Accounting of Disclosures Form.

Form available at www.privacy.utah.edu/forms

HIPAA § 164.514
How We Use and Disclose PHI

Use and Disclosure of PHI for Patient Care
Sharing PHI with a Patient’s Family

• When family/ friends/ caregivers accompany a patient to UUH...health information may be shared:

  – If we **ASK** the patient and they give their oral consent/ authorization;
  – If the **patient does not actively object**;
  – If circumstances indicate that the patient does not object;
  – If the family/ friend/ care facility representative are going to be **involved in the patient’s care outside of UUH**, and are given only the **amount of information necessary to care for the patient**.

**HIPAA § 164.510**
Patient Directory

• All patients admitted to UUH for services are automatically listed in the patient directory
  • If caller asks for patient by name we can provide:
    • Room Number, Condition (Critical, Serious, Stable, Good)
  • A patient may opt-out. If they opt-out:
    1. They will not appear in our patient directory if someone calls for them;
    2. We will not even acknowledge that they are in our facility

*Note:* A provider may opt a patient out if, in their professional judgment, it is in the best interest of the patient

**Check with your department for protocol on how to handle patients who have opted-out.**

Forms available at [www.privacy.utah.edu/forms](http://www.privacy.utah.edu/forms)

HIPAA § 165.510)
Patient Rights

• Aside from Treatment, Payment and Healthcare Operations (TPO), and Special Situations, patients must give Authorization IN WRITING for all other disclosures of their PHI, including...

  – Marketing
  – Selling PHI
  – Psychotherapy Notes
  – Drug & Alcohol Treatment Records (written patient authorization or special court order is required)

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

Patient authorization form is available at:
http://privacy.utah.edu/forms/
Patient Rights

• Patients can request to inspect and obtain a copy of their records
  – In paper or electronic format*
  – Only nominal fees may be charged to the patient to cover copy expenses or cost of CD/USB drive

• Accounting of Disclosures
  – Patients may request a list (accounting) of disclosures of their information (not including disclosures for treatment, payment and/or healthcare operations).

There’s a form for these requests!!
www.privacy.utah.edu/forms

*Send these requests to Health Information (Medical Records) 801-581-2704
Patient Rights

• Request Amendments to Medical Record
  – Patients may request a correction to their medical record they think is incorrect or incomplete.

• Request Restrictions
  – UUH does not have to honor all requests for restrictions....Except For...

• “Out-of-Pocket” Restriction
  ➢ If a patient pays for a service or health care item out-of-pocket in full, they can request, in writing, not to share that information with their health insurer.

There’s a form for these requests!!
www.privacy.utah.edu/forms
Patient Rights

• Request a Paper Copy of the Notice of Privacy Practices

• Request Confidential Communications
  – Patients can ask us to contact them in a specific way

• File a Complaint
  – Information about the UUH complaint process and right to escalate a complaint to Health and Human Services (HHS) can also be found in the ‘Notice’

• PHI Breach Notification
  – We must let patients know promptly if their health information has been compromised

There’s a form for patient requests!!
www.privacy.utah.edu/forms
Employee Access to PHI
Employee 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 family members, co-workers, friends, supervisors, high profile patients, etc., unless you are part of the care team.

UUH employees 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 access family members’ health records.

Questions regarding release of PHI?
Contact Health Information (Medical Records) 801-581-2704
Employee Access to Minor Children's PHI

UUH employees may not directly access the records of your children (any age) in the EMR...

**BECAUSE**...Utah State Law allows minors to consent to treatment for reproductive issues and sexually transmitted diseases (STDs). They are entitled to have that health information kept private and not released without their authorization.

**To get your children's records...**

Go to the Health Information Department (HI), complete and sign an authorization, and HI personnel may allow you access your children's’ 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 these 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 an @utah.edu 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.
Issues With PHI Data Disclosures
Issues With PHI Data Disclosures

• In order to be compliant with HIPAA Law:
  – **ANY** suspected *breach, loss or disclosure involving protected health information* (PHI) must be reported no later than 24 hours after the discovery of the incident.
  
  – This applies to protected health information (PHI) used in all settings:
    • Administrative
    • Operational
    • Clinical
    • Academic
    • Research

☞ Report to the Hospital Help Desk (587-6000)

**NOTE:**

HIPAA requires notification to each affected patient or individual if an unauthorized disclosure of PHI is discovered.
Examples of Unauthorized Disclosures

• Faxes containing PHI mistakenly sent to the wrong fax machine outside UUH.
• Accessing PHI without a business “need to know.”
• Lost or stolen unencrypted USB/thumb drive containing PHI.
• Lost or stolen unencrypted laptop containing PHI.
• PHI being sent to the wrong individual/patient.
• Paper PHI not shredded.
• Emails containing PHI sent unencrypted to the wrong email address outside UUH.
• Any unprotected and/or unencrypted PHI sent outside UUH.
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.

HIPAA, Safeguards & University of Utah Policies and Procedures
Report Unauthorized Disclosures

If you discover a potential disclosure, or if you become aware you or a co-worker are not following information security policies...

Call for Assistance! Call to Report!

- **Report** it to the Hospital Help Desk at 801-587-6000 immediately.

- **Complete an incident report at:** [www.privacy.utah.edu](http://www.privacy.utah.edu)

- Privacy personnel will be notified and will help you determine if patient notification is required.

*University of Utah Policies and Procedures*
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 privacy and security issues.

*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

*HIPAA § 160.103; § 164.504*
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.

HIPAA § 164.504
Business Associates (cont.)

For a current list of contracted Business Associates (BAs):

http://privacy.utah.edu/intranet/files/uUUH-ba.xls

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

HIPAA § 164.504
BAs, Vendors, Volunteers, Visitors and Shadowers
BAs, Vendors, Volunteers & Shadowers

Business Associates, Vendors, Volunteers, Visitors (who are not patients and/or not accompanying or visiting patients), and Shadowers are only allowed in any UUH Patient Care Area(s) when:

– They have **signed** a UUH Confidentiality and Security Agreement

– They have **completed** required UUH HIPAA Privacy and Security training

– They are **identified** with a controlled UUH ID badge

Individuals “shadowing” health care professionals or observing patient care must also have a sponsor, a complete and approved shadowing form and permission from the sponsor’s direct supervisor.
Violations and Sanctions

(Sanctions = Consequences)
University of Utah and UUH penalties apply, up to and including termination, if there is a willful disregard to policies and/or if confidentiality or security of private information is knowingly breached.

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 **Accounts** and/or improper use of **Computers**. **Examples** may include but are not limited to:

- **Sharing accounts**, posting or giving out personal **password or account** access information

- **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](http://www.privacy.utah.edu) > “Report an Incident”. Your report will remain confidential.
Violations Include...

- Getting into personal 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) without authorization

- 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 U of U/UUH

– **Selling** health or personal information; or inappropriately selling/giving such information to the news media

– **Transporting or photocopying** paper protected health information and/or **taking it home** without authorization and/or without de-identifying the data
Consequences Can Include...

U of U and UUH sanctions for violations can include:

- Verbal counseling and warnings
- Letters of reprimand
- Loss of access to computer systems
- Suspension, termination of employment, or expulsion from University of Utah/UUH
- Loss of faculty appointment and/or student privileges
- Reporting to professional licensing or credentialing boards

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 § 164.530
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

  (HIPAA § 160.308)

• “Enhanced Enforcement,” as listed in HIPAA, permits State Attorneys General to pursue civil actions

  (HIPAA § 160.404; 160.408)

• Mandatory monetary penalties will be imposed for “willful neglect” of privacy and security

  (HIPAA [see next slide])
HIPAA Monetary Penalties

- **“Violation Occurred after Reasonable Precautions”**
  - Minimum Penalty: $100
  - Maximum Penalty: $1,500,000

- **“Violation Resulted from Reasonable Cause”**
  - Minimum Penalty: $1,000
  - Maximum Penalty: $1,500,000

- **“Willful Neglect – Corrected Within 30 Days”**
  - Minimum Penalty: $10,000
  - Automatic Government Audit
  - Maximum Penalty: $1,500,000

- **“Willful Neglect – Uncorrected Violation”**
  - Minimum Penalty: $50,000
  - Automatic Government Audit
  - Maximum Penalty: $1,500,000

Due Diligence

Due Diligence

HITECH
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
Questions and/or to Report Incidents

Privacy and Security Reports

– Confidential privacy breach reports, a privacy complaint, to report a privacy and/or security incident, or if you have any privacy questions:

• Online - http://www.privacy.utah.edu > Report an Incident

• The Hospital Help Desk at 801-587-6000

ALL reports and complaints are confidential and are thoroughly investigated

HIPAA § 164.530
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
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 Shadowers, Vendors 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 ___________________________