The Health Insurance Portability & Accountability Act (HIPAA)

University of Wyoming Office of General Counsel

- Deputy General Counsel, Paula Whaley
- Senior Associate General Counsel and Chief Risk Officer, Laura Betzold

UNIVERSITY OF WYOMING

Disclaimer

- This training only provides a high-level overview of HIPAA and does not cover ALL the requirements under HIPAA.

- More detailed information about HIPAA from the U.S. Department of Health and Human Services (HHS) can be found at HHS HIPAA for Professionals and HHS Professionals FAQ

What is HIPAA?

- HIPAA is a set of federal laws and regulations (or Rules) that apply to health records and other personally identifiable health information.
- While HIPAA applies to many businesses, what's important for the University of Wyoming is the **Privacy Rule**

  - "The HIPAA Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization."

  - "The rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."

The Law

- HIPAA is overseen by the Department of Health & Human Services (HHS)
- The Regulations include provisions on:
  - Privacy of health information (Privacy Rule)
  - Security of health information (Security Rule)
  - Notification of breaches of confidentiality (Breach Notification Rule)
  - Penalties

What Does HIPAA Protect?

- Under the Privacy Rule, HIPAA protects **Protected Health Information (PHI)**
- **PHI** includes:
  - Individually identifiable health information that is:
    - Transmitted by electronic media;
    - Maintained in electronic media; or
    - Transmitted or maintained in any other form or medium.
    - Some common examples include: medical charts, photographs, communications between health care professionals, billing records, health plan claims records and insurance policy numbers.
    - Includes common identifiers such as an individual's name, address, birth date, and Social Security Number.

- **PHI** does **NOT** include:
  - Education records covered by the Family Educational Rights and Privacy Act (FERPA).
  - Information regarding a person who has been deceased for more than 50 years.

To Whom Does HIPAA Apply?

- HIPAA mainly applies to **covered entities** and **business associates.**
- **Covered entities** are:
  - Health care providers that electronically transmit health information within the requirements of HIPAA
  - Health plans (with some exceptions)
  - Health care clearinghouses
- **Business associates** are:
  - People or organizations that provide services to or perform services on behalf of a covered entity

What Does HIPAA Mean For You?

- If you are part of a covered entity you are prohibited from disclosing PHI to any third parties, unless the individual who is the subject of the information (or that person's personal representative) authorizes it in writing or the rule otherwise permits the disclosure. You must be familiar with and abide by your covered entity's specific HIPAA policies and procedures.
- Covered entities must:
  - Have policies and procedures in place in compliance with both the Privacy and Security Rules
  - Have a public Privacy Notice and designated Privacy Officer
  - Train their workforce regularly on the HIPAA Policies and Procedures
  - Have safeguards in place to protect the confidentiality of PHI
  - Report and investigate breaches

Is the University of Wyoming a Covered Entity under HIPAA?

- We are a **Hybrid Entity**
  - A **Hybrid Entity** is an entity that conducts both covered and noncovered activities. This means that the University has designated which components of the University (Healthcare Components) fall under HIPPA. All others do not.

- **The following are the regular HIPPA Healthcare Components at UW (not including business associates)**
  - **The UW Family Medicine Residency Programs (Cheyenne and Casper locations) and the Albany County Community Health Clinic**
  - **The UW Speech and Hearing Clinic**
  - **Wyoming Institute for Disabilities**

UW Covered Entities and HIPAA Policies

- UW has general HIPAA policies that each Healthcare Component of our hybrid model must follow
- However, each Healthcare Component will also have their site-specific policies to supplement and complement the general policies. This is important because no site has exactly the same physical components or technology.
- Site specific policies need to be tailored to the site to maximize privacy and security and must be reviewed and approved by the UW Privacy and Security Officers.

Are any uses of PHI permitted without the individual's consent?

- There are a number of exceptions that allow a covered entity to disclose PHI without having express consent from the individual. These are listed in the Regulation, but some common categories include:

  - Treatment, Payment, or Health Care Operations
    - Example: A health care provider may disclose PHI about an individual as part of a claim for payment to a health plan.
    - Example: A health care provider shares PHI with a treating physician from a specialty clinic.

  - Disclosure is Required by Law or for Law Enforcement Purposes
    - Example: The health care provider receives a court order requiring disclosure.
    - Example: The health care provider is asked by law enforcement for information about a victim or suspected victim of a crime.

What does the Security Rule require of covered entities?

- The Security Rule requires regular risk assessments of its safeguards and provides regulatory requirements for covered entities to meet certain security standards in the areas of:
  - Administrative safeguards
    - Example: assigning security responsibility to an individual and requiring training
  - Physical safeguards
    - Example: Restricting to electronic PHI and retaining off site computer backups
  - Technical safeguards
    - Example: Encrypting electronic PHI as it is being stored and/or transmitted

What types of things can you do to safeguard PHI?

- Do not access PHI that you do not need.
- Send PHI encrypted when sending electronically.
- Turn computer monitors away from public viewing and do not leave them unlocked when unattended.
- Do not leave PHI in unsecured areas, such as shared printers.
- Use a low voice when speaking about PHI and avoid discussing PHI around those who do not need to know.
- Use strong passwords.
- Do not open attachments to emails unless from a trusted source.
- Shred hard copies when no longer needed.
- **Report any possible or suspected breaches of HIPAA to your supervisor or Privacy Officer immediately.**

Identifying a Potential Breach of HIPAA

- **Breach:** The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.
    - Potential Breach Example 1: An exam room computer was left logged in and open and an unauthorized user viewed electronic health records of patients.
    - Potential Breach Example 2: A doctor clicked on a suspicious link in an email and her account was compromised and an outside entity could have access to PHI.

What are the Potential Penalties for violating HIPAA?

- Disciplinary Action
- Civil Penalties
- Criminal Penalties
- Lawsuits

Questions?

Contact Information

Current UW Privacy Officer:
Patrick Hardigan, Dean, College of Health Sciences
phardiga@uwyo.edu

Current UW Security Officer:
Amy Mclaughlin, Vice President and Chief Information Officer, Information Technology
amy.mclaughlin@uwyo.edu