Contents

Q = Content relevent to quiz

HIPAA Overview

To improve the efficiency and effectiveness of the health care system, the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 was passed as Public Law 104-191. The department of Health and Human Services, Office of Civil Rights, administers and enforces the law.

HIPAA was created to:

- Provide continuity and portability
- Combat fraud and abuse
- Provide uniform standards
- Reduce administrative expenses and
- Ensure security and privacy

There are two sets of standards within HIPAA

- Privacy Standard
- Security Standard

Each talks about a different set of activities related to keeping health information safe.

Who must comply?

HIPAA defines organizations that work with health information as Covered Entities (C.E.s). These include:

- Health Plans
- Healthcare providers (including mental health providers)
- Healthcare Clearing Houses

Who Must Comply at ASU?

- Any department within ASU that has been identified as part of the Covered Entity must comply with HIPAA.
- Any department that does not meet the requirements for a Covered Entity but handles Protected Health Information (PHI) should also comply with HIPAA standards.
- Any ASU employee who provides management, administrative, financial, legal or operational support to a Covered Entity at ASU must comply with HIPAA.

Business Associates (B.A.) must also comply with HIPAA. B.A.s may include:

- Other Covered Entities
- Anyone who performs certain functions or activities that involve the use or disclose of Protected Health Information (PHI) on behalf of, or provides services to, a covered entity.
- Anyone who maintains PHI on behalf of a covered entity, even if they don't have access to the actual protected health information.

Q = Content relevent to quiz

Covered Entities should create a Business Associate Agreement (BAA) with all Business Associates that outlines the nature of their relationship and the PHI to which the BA has access.

ASU has a Business Associate Agreement template that all members of the ASU Covered Entity should use for their Business Associates.

Business Associates are held responsible to the same standard of compliance as members of the Covered Entity: Q

- B.A.s are liable for violations of the security and privacy rules
- B.A.s must report Covered Entity (CE) breaches of unsecured PHI
- B.A.s are prohibited from retaliating for actions related to HIPAA compliance
- B.A. compliance and liability also apply to sub- contractors
- If disclosing to another health care provider for the purpose of patient treatment, a B.A. agreement may not be needed.
- B.A. agreements must include new obligations as outlined in the Omnibus Rule of 2013.

Business Associates can cover a wide range of people and companies. Some examples include:

- External record copying/transcription services
- External storage and retrieval services
- External collection services
- External delivery/courier services
- External business consultants
- Any sub-contractor that creates, receives, maintains or transmits EPHI on behalf of a business associate.

Privacy Standard

The privacy standard talks about what information should be private and how to manage it. The major concepts of the standard are listed here.

Protected Health Information (PHI) Q

Protected Health Information is individually identifiable information that is:

- the past, present, or future physical or mental condition of an individual
- documentation of the provision of healthcare to an individual
- payment or records of payment for care provided to an individual
- used to identify the individual (Includes at least one of the 18 personal identifiers)
- transmitted or maintained in any form (electronic, paper, or orally)

Q = Content relevent to quiz

There are 18 identifiers that would qualify any information has PHI, whether it is presented in electronic or hard copy format. The 18 identifiers are:

- Name
- Postal address
- All elements of dates except year (age is not an identifier unless over 89 years)
- Telephone number
- Fax number
- Email address
- URL address
- IP address
- Social security number
- License numbers
- Account numbers
- Medical record number
- Health plan beneficiary #
- Device identifiers and their serial numbers
- Vehicle identifiers and serial number
- Biometric identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic

If ANY of this information is included in a form or document, the entire document becomes Protected Health Information (PHI).

When a document is adequately "de-identified", it is no longer considered PHI. Complete de-identification requires the removal of all 18 identifiers.

Minimum Necessary Rule

When sharing information, PHI must be shared ONLY with agencies and individuals who have a need for the information. Only the minimum amount of information required should be released.

Where disclosures are required by Arizona state statutes, the Privacy Rule's minimum necessary standard does not apply, because the law requiring the disclosure will establish the limits on what should be disclosed.

= Content relevent to quiz

Requests for PHI

- Each Covered Entity must have certain staff members designated to disclose and/or use PHI. ALL uses and disclosures of PHI must be processed by the personnel designated by the unit's HIPAA Privacy Officer.
- When a Covered Entity receives a request for PHI, the requestor's identity and authority to receive PHI must be verified (the identity of patient must also be verified when he/she is requesting their records).
- Requests for PHI require patient authorization to release information (with some exceptions).

Acceptable PHI Releases

There are certain times when the release of PHI does not require a Release of information (ROI).

- When requested by the patient
- When requested by the Office of Civil Rights to enforce HIPAA Privacy Standards
- For treatment or payment purposes
  - Includes communication with patient's family when in best interest of patient and information is limited to that needed for family participation in patient care
- For healthcare operations, including:
  - Quality assessment or peer review activities
  - Accreditation
  - Training
  - Business administrative functions

Decedent's PHI must:

- Be protected for 50 years following their death.
- After 50 years, information is no longer considered PHI
- CE may disclose to others besides personal representatives if they are involved in the person's care.

Special Circumstances

Note: Consult with your unit's HIPAA Privacy Officer following requests for PHI to ensure compliance with HIPAA Privacy Standards & ASU Policy.

There are times when disclosure of PHI does NOT require patient approval.

Q = Content relevent to quiz

Public purposes:

- Health oversight activities:
  - Audits; civil, administrative or criminal proceedings; oversight of health care system, government benefit programs, civil rights laws
- Public health activities:
  - Communicable disease reporting
  - Child/dependent abuse reporting
  - Federal Drug Administration (FDA) reporting
  - Workers compensation
  - Immunization data entry into Arizona State Immunization System (ASIS) for students up to age 18 (allowed under state law)

Law enforcement

- For identifying a suspect, fugitive, material witness or missing person
- Per request of law enforcement official for information about an individual who is or is suspected to be a victim of a crime
- As required by a specific state or federal law

Judicial and administrative hearings

- Court order
- Subpoena, discovery request or other lawful process when authorization is provided by patient (or when reasonable assurances are provided by requestor that efforts have been made to inform the patient of the request)

Decedent records

- To funeral directors as needed to carry out duties, for example.

For specialized government functions:

- Military and veterans activities
- National security and intelligence activities
- Protective services for U.S. president and other government officials
- Department of State medical suitability determinations
- Corrections institutions
- Government programs providing public benefits
- To avert a serious threat to the health and safety of society

For research purposes under following conditions:

- Board approval of waiver of patient authorization
- Documentation of research purpose is provided
- Privacy of patient is maintained in findings

At all other times, the disclosure of PHI requires patient authorization.

 = Content relevent to quiz

Rules for Marketing or Sale of PHI

There are rules about using PHI for marketing or sales purposes:

- Patient must grant permission to market to the patient
- Disclosure that the 3rd party is paying the Covered Entity to market to the patient must be made to the patient.

"Sale of PHI" is defined as:

- The receipt by a Covered Entity (CE) or Business Associate (BA) of direct or indirect financial or non-financial remuneration in exchange for PHI.
- Patient authorization must state that the Covered Entity will receive remuneration
- **Does NOT include:**
  - Public health purposes, research (non-profit), or assessing fees to a patient to access or disclose their own PHI.

Patient Authorizations

A valid Patient Authorization must:

- Be written in plain language
- Be signed by the patient
- A copy of the signed patient authorization must be provided to the patient.

A valid patient authorization must include the following information:

- Type of PHI to be used or disclosed
- Purpose of disclosure
- Name of person or entity receiving PHI
- Notice of potential re-disclosure of PHI by recipient
- Date authorization expires
- Patient right to revoke authorization in writing
- Statement regarding ability and inability to make treatment, payment, enrollment or eligibility as a condition of patient authorization

 = Content relevent to quiz

Patients' Rights

Patients have the right to:

- Access their "designated record set" which may include:
  - Documents used to make healthcare decisions
  - Billing records
  - Enrollment, payment claims, and case or medical management record systems
- Obtain an accounting of any/all disclosures of their PHI
- Request restrictions of the use/disclosure of their PHI
- Authorize non-treatment uses/disclosures of their PHI with authorization
- Request an amendment to their record
  - The Covered Entity (CE) may deny this request if it believes the record is accurate and complete or if it was not the creator of the record.
- File a complaint to the Secretary of the Department of Health and Human Services (DHHS) and the Covered Entity (CE)
  - At ASU, individual units must notify the University HIPAA Privacy and Security Officers of all patient complaints
- Request alternative channels of communication
- Receive a Notice of Privacy Practices (NPP) at their first and any subsequent visits. The Notice of Privacy Practices must also be posted in a location convenient for the patient to review.
- Receive Electronic Records
  - Patients may request to get a copy of their records from the electronic designated record set if it is readily producible.
  - Covered Entities may charge fees for providing an electronic copy, including charging for portable media devices (e.g. a thumb drive).
- Receive Email
  - B.As and C.E.s can send unencrypted PHI to individuals if the individual is warned and agrees.
  - ASU's Data Handling Standard prohibits sending unencrypted PHI via email. When ASU's standards and the HIPAA rules don't agree, consult your local HIPAA officer.
- Request to restrict disclosure of their PHI to a health plan if:
  - The disclosure is for the purpose of carrying out payment or health care operations and is not required by law; and
  - The PHI only pertains to an item or service for which the individual has paid in full.
- Receive notification if a covered entity is receiving remuneration for marketing activities. Patient permission is required for marketing activities.
- Be provided with clear and conspicuous Opt-Out provisions for all fundraising activities by a Covered Entity.
  - Opt back in once they have chosen to opt-out.
  - A Covered Entity cannot condition treatment or payment based on opting-in for fundraising activities.

= Content relevent to quiz

Privacy Rule Administrative Requirements

Each Covered Entity must:

- Appoint a HIPAA Privacy Officer
- Develop and implement Privacy policies
- Provide annual HIPAA training to their staff
- Implement policies and procedures for responding to complaints
- Adopt sanctions for workplace violations of HIPAA policies
- Mitigate damage to patients resulting from violations
- Provide each client with a Notice of Privacy Practices.
- Post the Notice of Privacy Practices where it is easily reviewed by each client.
- Obtain documentation from each client that they were provided with a Notice of Privacy Practices.

Notice of Privacy Practices (NPP)

The Notice of Privacy Practices must:

- Be written in plain language
- Include a standard header
- Describe standard uses and disclosures of PHI
- Describe each individual's rights regarding PHI
- Describe the Covered Entity's duties
- Describe how a patient can place a formal complaint
- Contain the effective date of the notice
- The Department of Health and Human Services provides sample Notices of Privacy Practices. These can be accessed at: https://www.hhs.gov/ocr/privacy/hipaa/modelnotes.html

= Content relevent to quiz

HIPAA Security Standards

The Security Standards are intended to:

- Ensure confidentiality, integrity, and availability of electronic PHI (ePHI)
- Protect against reasonably anticipated threats or hazards to the security and integrity of PHI and ePHI
- Protect against unauthorized uses/disclosures of PHI and ePHI
- Ensure the implementation of workplace training and compliance

There are three types of safeguards

- Administrative safeguards
  - policies and procedures to protect PHI (includes training of employees who handle PHI and disciplinary policies for unauthorized use/disclosure of PHI)
- Physical safeguards
  - physical security of facilities housing PHI and electronic media and hardware housing electronic PHI
- Technical safeguards
  - electronic security of PHI (e.g., encryption, passwords, automatic log-offs, screen protectors, access tracking)
  -

Administrative Safeguards

Administrative safeguards include these actions:

- Implement policies/procedures to prevent, detect, contain and correct security violations
- Identify a HIPAA Security Officer responsible for development and implementation of security policies and procedures
- Authorize appropriate "role-based" access to PHI for each employee (includes terminating access to ePHI at end of employment)
- Implement policies/procedures for authorization of access to PHI
- Ensure employees receive HIPAA training prior to receiving access to PHI and annual HIPAA training thereafter
- Obtain assurance that business associates will properly safeguard PHI
- Develop policies/procedures for addressing security incidents
- Review and maintain security policies, procedures and systems
- Establish policies/procedures for responding to an emergency or other incident that damages systems containing ePHI
- Data back-up
- Disaster recovery
- Emergency mode operation to ensure continual protection of ePHI

= Content relevent to quiz

Physical Safeguards

- Verbal Security (No conversations about patients in public places)
- When sharing PHI via telephone, verify the identity of the other party
- PHI should not be left on voice mail or answering machines unless the patient has authorized to do so
- Use noise suppression and/or radio to mask sounds
- Office security
    - Only authorized employees should have access to areas that contain PHI
    - Use a secured enclosure (e.g., locked cabinet or desk) for paper records
    - Lock offices when vacant
    - When printing PHI, be physically present at the printer unless the printer is in a secured area
    - Use secure fax machines* and specify restrictions of use/disclosure of PHI on the faxed documents

  * Dedicated fax machine on non-shared analog phone line only
- Disposal of PHI
    - Shred paper documents
    - Erase data and physically destroy electronic media devices housing ePHI (e.g., flash drives, copiers)
- Ensure desktop monitors are not visible by unauthorized individuals and use screen protectors on computer monitors
- When mailing PHI, use a sealed envelope clearly labeled "confidential" or "Protected Health Information – To be opened by Addressee Only"
- Log off from or lock computer when not at workstation
- If using a shared workstation, log off before walking away and before others use workstation
- Secure laptops and portable media devices with locking cable when unattended
- Maintain a record of relocation/disposal of hardware and media devices containing ePHI
- Store PDAs, memory sticks and other portable devices in locked and secured areas
- Report lost or stolen media devices containing PHI
- Notify your unit's Information Security Officer and the University Information Security Office if you suspect unauthorized access of your workstation

= Content relevent to quiz

Technical Safeguards

- System Access/Authorization Control
  - Assign a unique User ID and password for authorized users
    - Never share your password
    - Do not post your password anywhere- memorize it
    - Use strong passwords (mix of upper and lower case letters, numbers and symbols)
    - Change password every 3 months
  - Do not set auto log-in on web browsers
  - Set computer to log-off after 10 minutes of inactivity
  - Save ePHI to a secure server - never on hard drive of computer
  - Do not install unauthorized software
  - Delete ePHI when no longer needed
  - User access to ePHI must be regularly audited to ensure appropriate access and use of ePHI
  - Use data loss prevention (DLP) software to ensure no ePHI is stored locally
  - Use antivirus and anti-malware software and set scans to run automatically
  - It is best to not store ePHI on portable devices, but if necessary, have data and passwords encrypted
- E-mail Security
  - E-mail is not a secure mode of communication - Do not include PHI in e-mail
  - Do not forward or reply to e-mail containing PHI
  - Do not open suspicious and/or non-work related attachments or those from unknown sources
  - Do not provide password or user ID via e-mail
  - Your department should use or develop secure ways to communicate with patients
- Workstation Hardening
  - HIPAA does not define a specific regimen of workstation hardening requirements specific to a platform or specific configuration standards. Multiple specifications in the safeguards provide opportunities for an entity to implement endpoint controls that demonstrate security over the entire environment. These may include (but are not limited to) the items listed next:

Q = Content relevent to quiz

- Suggested Workstation Hardening Specifications:
  - Segmentation of workstations used to enter ePHI from other systems – not explicitly linked to a specification, but logical to implement given need to limit access over network to systems involved in ePHI scope
  - Centralized Logging and Monitoring (Log-in Monitoring: CFR 164.308 (a)(5)(ii)(C); Logging: CFR 164.312(b); Information System Activity Review: CFR 164.308(a)(1)(ii)(D))
  - Centralized Anti-Virus (Protection from Malicious Software: CFR 164.308(a)(5)(ii)(B))
  - Endpoint Encryption of whole disk or individual systems resources (Encryption and Decryption: CFR 164.312(a)(2)(iv))
  - File Integrity Monitoring (Integrity: 164.312(c)(1))
  - Patch and Vulnerability Management – effectively an extension of Protection from Malicious Software requirements using a defense in depth strategy)

Centralized Organization

ASU has a central HIPAA compliance structure

ASU HIPAA Privacy Officer: Aaron Krasnow
Assistant Vice President/Director
ASU Counseling Services
ASU Health Services
aaron.krasnow@asu.edu

ASU HIPAA Security Officer: Tina Thorstenson
Associate Vice President
Chief Information Security Officer
tina.thorstenson@asu.edu

Unit Privacy and Security Officers

- Each Covered Entity at ASU has the responsibility to assign a local HIPAA Privacy Officer and HIPAA Security Officer.
- These individuals are responsible for ensuring HIPAA compliance for their individual units, and for communicating with the University HIPAA Privacy and Security officers when there are complaints, breaches, concerns or other possible HIPAA compliance issues.

ASU Data Handling Standard

- Housed on the UTO Policy page: uto.asu.edu/policy
- Defines 4 data sensitivity levels

Q = Content relevent to quiz

Breaches

What is a breach?

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

UNLESS

The Covered Entity or Business Associate can demonstrate based on a risk assessment a "low probability" that the PHI has been compromised

Examples of a breach

- Laptop containing PHI is stolen
- Memory stick containing PHI is lost
- Receptionist who is not authorized to access PHI looks through patient files in order to learn of a person's treatment
- Computer hacking
- Client records are removed from an unsecured fax machine by an unauthorized individual

Disclosures that are NOT considered to be a breach

- Inadvertent disclosures of PHI from one authorized person to another.
  e.g. A staff member not treating a patient overhears a conversation regarding the patient's treatment plan
- Unintentional acquisition, access, use or disclosure by a workforce member acting under the authority of a Covered Entity (CE) or Business Associate (BA) - Includes volunteers, trainees, and other persons under the direct control of the entity, whether or not they are paid by the Covered Entity
  e.g. A trainee accidentally opens the clinical file of the wrong patient and begins to read the record before realizing he is seeking information on a different patient.
- A use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure
  e.g., calling out a patient name in the waiting room

= Content relevent to quiz

How to determine if it was a breach

A Risk Assessment must be conducted for every unauthorized access, use or disclosure of PHI to determine if a breach occurred.

Risk Assessment Factors:

- Nature and Extent of PHI
- Who got the information
- Extent to which the risk has been mitigated
- Whether PHI actually was acquired or viewed

Risk Assessment example

An employee leaves the university and access to systems including PHI was never removed:

- Nature and Extent of PHI
  - likely high risk
- Who got the information
  - potentially the former employee, high risk
- Extent to which the risk has been mitigated
  - little use if the employee can access remotely
- Whether PHI actually was acquired or viewed
  - demonstrate through log files that the user never accessed the information

Reporting standards for breach notifications

HIPAA standards require you to notify your unit's HIPAA Privacy or Security Officer AND The University Privacy and Security Officers

- HIPAA Standards require individuals to be notified when their PHI has been inappropriately disclosed
  - Employees must report breaches to their unit's Security Officer who will lead the notification process in consultation with the University Security Officer
  - Notification must be made without unreasonable delay (and within 60 days of breach)
  - These notifications are done in consultation with the ASU Information Security Office (infosec@asu.edu)

Breach Notification to individuals must contain

- A brief description of what happened, including the date of the breach
- A description of the types of unsecured PHI that were involved in the breach
- Any steps individuals should take to protect themselves from potential harm
- A brief description of what the Covered Entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches
- Contact information for individuals to ask questions

Q = Content relevent to quiz

Reporting Breaches

- Breaches of privacy and security standards must be logged and submitted to the Department of Health and Human Services (DHHS)
- DHHS lists breaches on a public website
- Prominent media outlets serving a state/jurisdiction must be notified of breaches affecting more than 500 residents of the state/jurisdiction

Disciplinary Actions for Breaches

Individuals who breach ASU HIPAA Policies will be subject to appropriate discipline under the unit's and ASU's policies

HIPAA Enforcement

The federal government imposes strict penalties on individuals and entities that violate HIPAA

- A knowing and wrongful disclosure of PHI can result in criminal penalties that include fines and imprisonment
- The Office of Civil Rights (OCR) now conducts random audits of Covered Entities and may eventually include Service Providers

Penalties

Criminal Penalties

- Persons who knowingly and in violation of the law obtain or disclose individually identifiable health information can be criminally liable.

Civil Penalties

- Tiered civil penalties range from $100 - $50,000 per violation. (up to $1.5 million per year for a violation of an identical requirement)

Penalties apply to both Covered Entities (CEs) and Business Associates (BAs)

Additional HIPAA information

Health and Human Services HIPAA website
http://www.hhs.gov/ocr/privacy

Q = Content relevent to quiz