HIPAA Compliance Training

Heritage Provider Network
&
Affiliated Medical Groups

Table of Contents

At the end of this training, please complete the quiz successfully to receive the "Certificate of Completion". The training is not complete until the certificate and quiz results are submitted to contact information listed on the certificate.

Key Terms and Acronyms

- **Privacy** – The right of an individual to keep his/her individual health information from being disclosed.
- **Use** – With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (Also see Part II, 45 CFR 164.50)
- **Disclose** – Release or divulgence of information by an entity to persons or organizations outside of that entity. (Also see Part II, 45 CFR 164.501)

Key Terms and Acronyms

- **Authorization** – The mechanism for obtaining consent from a patient for the use and disclosure of health information for a purpose that is not treatment, payment or health care operations. For example, Protected Health Information (PHI) released for special Olympics activity.
- **Minimum Necessary** – When using any PHI, an entity must generally make reasonable efforts to limit itself to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."
- **Covered Entity** – Defined as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

What is HIPAA?

Health Insurance Portability and Accountability Act of 1996 &
Health Information Technology for Economic and Clinical Health Act of 2009 (Federal Law)

Portability:

- Protects and guarantees health insurance coverage when an employee changes job.
- Establishes national standards for electronic data transmission portability: Transactions (Enrollment, Eligibility, Claims, Payment and others), code-sets and identifiers.

What is HIPAA?

Health Insurance Portability and Accountability Act of 1996 &
Health Information Technology for Economic and Clinical Health Act of 2009 (Federal Law)

Accountability:

- Protects health data integrity, confidentiality and availability.
- Administrative simplification: Reduces fraud and abuse, makes fraud prosecution easier (Medicare/Medicaid).
- Establishes standards for protection of health information
  - Privacy (operational, consumer control, administration)
  - Security (administrative, physical, technical, network)

What is HIPAA?

Health Insurance Portability and Accountability Act of 1996 &
Health Information Technology for Economic and Clinical Health Act of 2009 (Federal Law)

Health Information Technology:

- Expands HIPAA to protect electronic PHI.
- Provides patients the right to obtain their PHI in electronic format.
- Requires notification of any unsecured breaches to appropriate entities (i.e. patients, Health Plans, HHS).

Privacy & Security

Privacy (example):

- Operational – Tracking of disclosures
- Consumer Control – Disclosure of patient rights
- Administration – Create policy and procedures

Security (example):

- Administrative – Contingency plans e.g. disaster recovery
- Physical – Facility access control
- Technical – Authentication
- Network – Data transmission security

Who is Affected by HIPAA?

- Employees who handle, use, or know individuals' Protected Health Information (PHI)
- Health Care Providers (health departments, hospitals, doctors' offices, any agency that transmits PHI electronically)
- Health plans that provide or pay the cost of medical care (*e.g.*, Medicaid, Medicare, CHAMPUS, BC/BS, HMOs)
- Trading Partners - Electronically exchange Protected Health Information
- Business associates - Perform services "on your behalf"
- HIPAA also applies to you as a consumer of healthcare!

HIPAA Enforcement

- **CIVIL PENALTIES for failure to comply**
  - $100 fine per person per violation
  - $25,000 fine per year for multiple violations
  - $25,000 fine cap per year per requirement
- **CRIMINAL PENALTIES for failure to comply**
  - Knowingly or wrongfully disclosing or receiving PHI: $50,000 fine and/or one year imprisonment
  - Commit offense under false pretenses: $100,000 fine and/or five years imprisonment
  - Intent to sell PHI or client lists for personal gain or malicious harm: $250,000 fine and/or ten years imprisonment

***You* can be *personally* liable, too!**

- These penalties apply to oral, paper and electronic Protected Health Information (PHI)

Protected Health Information (PHI)

(45CFR § 160.103)

- All individually identifiable health information (including demographic information, physical or mental health or other information that identifies the individual)
- Other information on treatment and care that is transmitted or maintained in any form or medium (electronic, paper, oral, etc.)

Examples of where PHI can be found:

- Medical records and billing records
- Insurance/Benefit enrollment and payment
- Claims adjudication
- Case or medical management

Examples of PHI

Unauthorized disclosure of any of the following, in conjunction with healthcare information will result in a HIPAA violation:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, etc.
- Telephone, fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, or characteristic

What is NOT Covered under PHI?

(45CFR § 160.103)

- Employment records of the employer
- Family Educational Rights and Privacy Act (FERPA) records

Preemption of state law:

Privacy Rule overrides any other state law unless that state law provides more protection for the consumer

De-identification of PHI

(45CFR § 164.514(a)(b))

Removal of certain identifiers so that the individual who is subject of the PHI may no longer be identified. Some ways to de-identify:

- Application of statistical method or
- Stripping of listed identifiers such as:
  - Names
  - Geographic subdivisions < state
  - All elements of dates
  - SSNs

For research, marketing and fund raising purposes, all PHI must be de-identified.

Some Ways of PHI Protection

- Close doors or draw privacy curtains/screens
- Conduct discussions so that others may not overhear them
- Don’t leave medical records where others can see them or access them
- Keep medical test results private
- PHI information should NOT be shared or be viewable in public areas
- Don’t leave copies of PHI at copy machines, printers, or fax machines
- Don’t leave PHI exposed in mail boxes or conference rooms
- Don’t share computer passwords or leave them visible
- Don’t leave computer files open when leaving unlocked or shared work area
- Dispose of paper containing PHI properly

Patient Rights Regarding PHI Disclosure

Patient rights regarding PHI disclosures:

- Receiving notice
- Requesting restrictions
- Accounting for disclosures
- Amendment
- Filing a complaint

Authorization issued for disclosure

- Must contain core elements and required statements, including:
  - Date or event that will trigger expiration
  - Statement that authorization is revocable

Patient Rights to Receive Notice

The patient has the right to receive a notice of privacy practices

Notice describes:

- How medical information is used and disclosed by an organization
- How to access and obtain a copy of their medical records
- A summary of patient rights under HIPAA
- How to file a complaint, and contact information for filing a complaint

Patient Rights to Request Restrictions

- The patient has the right to request an organization to restrict the use and disclosure (release) of his/her confidential information
  - Can request restriction in the use of information for treatment, payment, or healthcare operation purposes
  - Organization is not required to agree with restriction(s)
- The patient can request to receive communication from the organization for any healthcare-related information by alternative means or locations

Patient Rights to File a Complaint

The patient has the right to file a complaint to the following if he or she believes privacy rights were violated*

- Individual within the organization
- The Secretary of the Department of Health and Human Services

** Organization must provide contact information for filing a complaint*

Patient Rights to Account for Disclosures

Patients have the right to request a list of when and where their confidential information was released

- A list of disclosures (releases) within past six years (starting in April 2003)
  - Date of disclosure
  - Name of person or entity who received information and address if known
  - Brief description of reason for disclosure
- Exceptions: Treatment, payment, or healthcare operations

Uses & Disclosures of PHI

(45CFR § 164.502(a))

General Rule

- An entity may not use or disclose PHI, except as permitted or required by privacy rule

Disclosures must be given:

- To individual when requested and required
- To HHS, to investigate or determine compliance with privacy rule

Notice of privacy practices

- Purpose: To provide the consumer with adequate notice of uses or disclosures of PHI
- Must be written in plain language and be provided at the time of the first service or assessment for eligibility
- Has to provide Privacy Officer contact information

Uses & Disclosures of PHI

Opportunity for Individual to Agree or Object

Facility/Hospital Directories – 45 CFR § 164.510(a)

- Must give the patient an opportunity to restrict or prohibit (can be oral) the use or disclosure of his/her name, location, general condition, and religious affiliation
- Emergency exception

Family, Friends, and Advocates – 45 CFR § 164.510(b)

- Must give the patient an opportunity to agree or object to:
  - Disclose PHI relevant to the person's involvement in care or payment to family, friends, or others identified by the patient
  - Notify of the patient's location, condition, or death to family, personal representatives, or another responsible for care
- When the patient is not present or incapacitated, the above uses and disclosures are permissible using professional judgment in the best interest of the patient

Uses & Disclosures of PHI

Public Policy requires disclosure of PHI, as required by law (45 CFR § 164.512(g)-(l))

- For public health
- About victims of abuse, neglect or domestic violence
- For health oversight activities
- For judicial and administrative proceedings
- For law enforcement purposes
- About decedents (to coroners, medical examiners, funeral directors)
- For cadaveric organ, eye or tissue donations
- For research purposes
- To avert a serious threat to health or safety
- For specialized government functions (military, veterans, national security, protective services, State Department, correctional)
- For workers' compensation

Top 10 Privacy & Security Practices

1. When in doubt, don't provide information
2. Log off before you walk away from your computer
3. Verify fax numbers before sending
4. Do not send e-mails or use the Internet unless the connection is secure and approved
5. Verify the identity of the caller before releasing confidential information
6. Never share your password with anyone
7. Maintain the security of all patient information in all its medium, like paper, electronic and oral
8. Discuss patient information in private locations
9. Access information on a need-to-know basis, only to do your job
10. Dispose of confidential information according to proper procedures (e.g., locked shred bins)

Arizona Priority Care™

One Goal. One Priority. Your Healthcare.

Please click the link below to start the test.

HIPAA/HITECH Compliance