Central Control HIPAA Training

What is HIPAA?

HIPAA is an acronym for Health Insurance Portability and Accountability Act of 1996. It requires that “protected health information” or PHI be protected and handled confidentially, which includes how PHI is stored, who can access PHI, how PHI is transmitted, and how PHI is used.

HIPAA has two important rules: Privacy & Security Rules

- **Privacy Rule**: to protect the privacy of PHI that can identify a specific individual or person

- **Security Rule**: to set national standards for protecting electronic PHI

Protected Health Information (PHI)

PHI refers to individually identifiable health information which can be linked to a particular individual or person.

- The individual's past, present, or future physical or mental health
- The provision of health care to the individual
- The past, present, or future payment for the provision of health care to the individual

Common identifiers and examples of health information include:

Common Identifiers

- Names
- Social Security Numbers
- Birth Dates
- Addresses

Examples

- Care Plans
- Wound Care Logs
- Admissions & Referral Forms
- Restraint Logs
- Incident Reports

Who is Covered

- **Healthcare Providers** – Any person or organization who furnishes, bills, or is paid for health care in the normal course of business, such as Nursing Homes, Hospitals, and ICF/MR's.
- **Healthcare Plans** – Any individual or group plan (or combination) that provides, or pays for the cost, of medical care, such as health insurance issuers (Blue Cross Blue Shield), HMOs, Group Health Plans, Medicare, Medicaid.
- **Healthcare Clearinghouse** – Any company that translates data content or format for another entity from non-standard to standard or vice-versa.

Business Associates

A person or entity that performs a function for a covered entity which involves the use or disclosure of PHI. Some examples include:

- Consultant
- Attorney
- Collection Agency
- Medical Transcriptionist

Permitted Uses and Disclosures

The Privacy Rule allows you to use or disclose PHI as follows:

- To the individual
- For treatment, such as disclosing PHI to other healthcare professionals caring for the individual
- For payment, such as claims billing, review services for coverage, or medical necessity
- For healthcare operations which are the day-to-day operations necessary for quality care. Examples include verifying documentation and determining the quality of care provided by clinicians.

Authorization Not Required

The following allows you to use or disclose PHI without the individual's authorization:

- As required by law
- For public health activities
- For victims of abuse, neglect, or domestic violence
- For health oversight activities
- For judicial and administrative proceedings
- For law enforcement purposes
- For information about decedents
- For cadaveric organ, eye, or tissue donation
- For research purposes
- To avert a serious threat to health or safety
- For specialized government functions

Authorized Uses and Disclosures Required

A signature from the individual or their personal representative is required to use PHI:

- For use and disclosure of psychotherapy notes
- For use and disclosures to third parties for marketing activities

Minimum Necessary: Limiting Uses and Disclosures

When using or disclosing PHI, you should use only the minimum amount required to achieve the purpose of the particular use or disclosure. Please note that disclosures for treatment do not apply to this requirement.

State Law

If the state law is more protective of the individual, then it takes precedence over HIPAA.

Privacy Rights

An individual has the right to:

- Receive a written notice describing your facility's privacy practices on the first date of service
- See or receive a copy of their medical record or other health information
- Request that any incorrect information in their file be changed
- Have PHI communicated to them by alternative means and at an alternative location to protect confidentiality
- Request restrictions to the use and disclosure of their PHI
- Request a history of disclosures of PHI for six years prior to the request
- File a complaint regarding any privacy concern or breach of privacy with your facility or Department of Health and Human Services (HHS)

Documentation

Documentation should be kept for six years from the date of its creation. If the State law requires a longer period of retention, then the State law will apply.

Keep Passwords Safe

Your password is private and personal. It is the connection to everything you access and save on your computer.

- Never write your password on a post it note and place it on your computer
- Passwords are for your individual use
- Never email you password
- Never ask someone for their password or give them yours
- Never reuse passwords
- Do not use a short password
- Remember, passwords are strongest when fresh – change them often! Passwords should be at least (8) characters with one uppercase letter, one lowercase letter, one number, and one symbol.
-

NOTE: ***If anyone logs on the computer using your password or gains access to the computer because you did not log out, you are responsible for their actions and could be disciplined, up to termination.***

Computer Security

You need to protect the computer(s) by:

- Never storing PHI on a computer
- Setting a screen saver password
- Always locking your computer when you are not using it. You can quickly lock your computer by pressing the Windows and “L” keys at the same time.
- If the computer is shared with others, always log off the computer when you step away. Otherwise, anyone passing by might gain access to PHI, they are not authorized to use.

What Happens to Those Who Do Not Comply

If you violate HIPAA, the following penalties can be enforced on the company:

Violation Category	Each Violation	Violations of an Identical Provision in a Calendar Year
• Did not know	$100 - $50,000	$1,500,000
• Reasonable Cause	$1,000 - $50,000	$1,500,000
• Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
• Willful Neglect – Not Corrected	$50,000	$1,500,000