Campbell County Health

Excellence Every Day

May 2021

HIPAA PRIVACY & SECURITY TRAINING

reviewed by Kim Johnson, RHIA, CCH Compliance and Risk Specialist

NAVIGATION:

Use the DOWN ARROW or PAGE DOWN keys on your keyboard to advance.

Use the UP ARROW or PAGE UP keys to go back.

COURSE COMPETENCIES

This presentation addresses the elements of maintaining the privacy and security of Protected Health Information (PHI).

- Define HIPAA
- Describe HIPAA identifiers
- Explain how to protect PHI and when to access PHI
- Restate that CCH employees are responsible for handling PHI appropriately

What is HIPAA?

HIPAA (Health Insurance Portability and Accountability Act) is a Federal Law that specified Administrative Simplification provisions that:

- Protect the privacy of patient information
- Provide for electronic and physical security of health and patient medical information
- Simplify billing and other transactions

Who does HIPAA apply to?

HIPAA rules apply to all individuals that have access to, maintain, hear, or view PHI

PHI

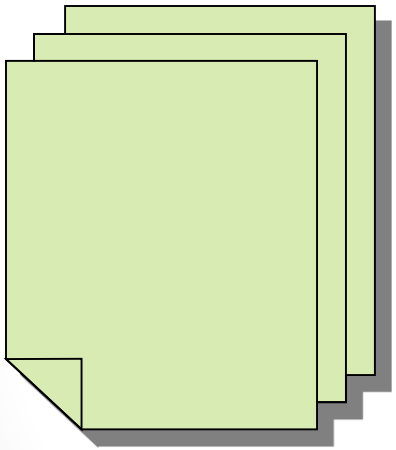
PHI or Protected Health Information is:

- Information about past, present, or future medical or mental health condition; created, or received by a provider in the course of treatment/evaluation in any medium.
- PHI excludes employment and research data; however these items are subject to other privacy laws and must be treated confidentially.

FORMS OF PHI

PHI exists in various forms:

Printed



Spoken

Electronic

It is the responsibility of every employee to protect the privacy and security of PHI in **all** forms.

Examples of PHI

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives
- Full face photographs or images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.

Causes of HIPAA Incidents

- Careless handling of PHI
- Unauthorized access or disclosure of PHI
- Sharing of Passwords
- Enabling another to work under the same user ID
- Accessing PHI without logging on with your information
- Failing to log off, shut off or otherwise protect the computer.
- Gossiping

Causes of HIPAA Incidents

- Faxing documents to wrong fax number
- Mailing reports or billing statements to wrong patient or address
- Giving documents to the wrong patient
- Leaving printed documents containing PHI unattended in public places
- Improper disposal of printed or written PHI
- Having storage devices unencrypted
- Sharing PHI while visitors are present in the patient's room without giving the patient the opportunity to object or consent

Use and Disclosures

Use:

The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company, or by a Business Associate of the Company.

Disclosure:

For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within CCH with a business need to know PHI.

Use and Disclosure

- Improper use or disclosure of sensitive information presents the risk of identity theft, invasion of privacy and can cause harm and embarrassment to Campbell County Health.
- Breaches of information can also result in criminal and civil penalties for both CCH and those individuals who improperly accessed or disclosed the PHI.

Every employee must protect the privacy and security of PHI.

Access Must be Authorized

An employee may only access, use or disclose PHI when this access is part of the employee's job.

Access

Employees may not access through any system or paper records information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes.

Your access to your own PHI or your child's PHI must be based on the same procedures other patients follow and not your access to the system for your job. For example, if you are awaiting lab results, you must follow the process to obtain those results by obtaining them through Health Information and Records (Medical Records).

Unauthorized Access

It is **never acceptable** for an employee to look at PHI just out of curiosity, even if no harm is intended (i.e. retrieving an address to send a card or viewing to see your neighbor's progress).

This is also true of accessing a high profile person, close friend, coworker's or family's record.

Access PHI only when needed to do your job.

If you are not providing care or performing part of your job duties, you should not be in the patient record.

These rules apply to all employees.

Breaches

A breach occurs when information that, by law, must be protected is:

- Lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for)
- Hacked into by unauthorized individuals
- Communicated or sent to others who have no official need to receive this PHI (i.e. gossip).

Minimum Necessary Standard

The **Minimum Necessary Standard** indicates:

- Staff have access to information that is based upon their job duties and roles.
- Staff should access only what they need to do their job.
- Staff should make reasonable efforts not to access, use or disclose more than the minimum amount of information needed to accomplish their job.

Minimum Necessary Standard

"PHI is confidential…

only access the minimum amount of PHI that

you need to know based on your job role…"

When do HIPPA rules apply?

- When you use it
- When you disclose it
- When you store it
- When you view it
- When it is lying on your desk or any desk
- When you share it with another healthcare provider
- When you talk about it face-to-face
- When you talk on the phone
- In all situations where PHI is present in any form.

Guidelines for Safeguarding PHI

Oral Conversations – in person

- Discuss participants PHI in private. Use an office with a door whenever possible, or leave areas where others can overhear.
- Be aware of those around you and lower your voice when discussing participants health information.
- If possible, point out health information on paper or on the screen.

Guidelines for Safeguarding PHI

Oral Conversations - telephone

- Follow the stated guidelines for “Oral Conversations – In Person”
- Don’t use names instead say; “I have a question about a patient”.
- Never give PHI over the phone when talking to an unknown caller, but call back and verify information.
- Never leave PHI on voice messages; instead leave a message requesting a return call to discuss a participant giving only your name and phone number.

Safeguarding PHI

Fax

- Use CCH cover sheet that includes the confidentiality statement, clearly identifying the intended recipient and include your name and contact information on the cover sheet.
- Do not include or reference PHI on cover sheet.
- Confirm fax number is correct before sending.
- Verify that fax was received by authorized recipient; check the transmission report to ensure correct number was reached and when necessary contact the authorized recipient to confirm receipt.
- Deliver received faxes to recipient as soon as possible.
- Do not leave faxes unattended at fax machine.

Safeguarding PHI

E-mail

- Do not include PHI in Subject Line of an e-mail.
- Utilize [SWD] Secure Web Delivery policy for sending confidential information outside of the CCH e-mail system.
- Include your contact information (name and phone number minimum) as part of the e-mail.

Courier and in-house Mail

- Use sealed, secured envelopes to send PHI.

Safeguarding PHI

Computer Workstations

- Do not share your password!
- Turn off the computer or log out of the network when not at your desk or the workstation.
- Position screens so they are not visible to others.
- Secure workstations and laptops with password.
- Do not leave laptop unsecured in a car, home office, or in any public areas.

Safeguarding PHI

Work Areas

- Do not leave PHI (files, records, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.
- Store all PHI securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area.
- Never remove original copies of PHI from CCH.

Disposal of PHI

- Shred all hard copies containing PHI when the copies are no longer needed, using the blue shred bins.
- Never throw PHI into a trash can.