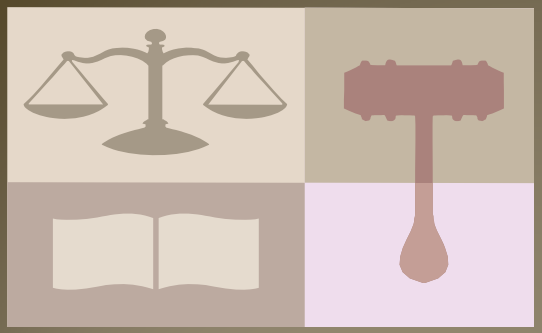
HIPAA Privacy and Security Training

Prepared by:
Bureau of Human Resources, Dept. of Health, Dept. of Human Services,
Dept. of Social Services, Bureau of Information and Telecommunications
Revised for EMS Use January 2016

HIPAA Education Objectives

- Overview of the requirements of HIPAA Final Rule
- What information must be protected
- How HIPAA affects you and your job
- Your responsibilities
    - Confidentiality
    - Computer Practices
    - Reporting Privacy Incidents & Security Breaches



What is HIPAA ?

The Health Insurance Portability and Accountability Act (HIPAA) is…

A federal law that specifies administrative simplification provisions that:

- Protect the privacy of patient / employee information
- Require “minimum necessary” use and disclosure
- Provide for security of patient / employee information
- Specify patient / employee rights to approve the access and use of their medical information

What does HIPAA cover ?

Privacy Rule

Compliance date: 04/14/2003

Security Rule

Compliance date: 04/21/2005

HITECH Act

Compliance date: 02/18/2009

HIPAA Final Rules

Compliance date: 09/23/2013

Definitions

HIPAA definitions

Business Associate

A person or entity that performs certain functions or activities involving the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a Business Associate.

Confidentiality

The protection of personal information, safeguarding it from unauthorized disclosure.

Covered entity

Generally, a health plan, health care provider or health care clearinghouse.

Disclosure

The release, transfer, provision of, access to or divulging in any other way information outside the entity holding the information.

HIPAA definitions

Privacy

The right of an individual to control his / her personal information and to not have it shared and used inappropriately by others.

Protected Health Information (PHI)

Individually identifiable health information, whether it is in electronic, paper or oral form, and is created or received by or on behalf of a covered entity or its Business Associates.

Security

The physical realm of data, and the integrity with which it is captured, stored, transmitted and protected.

Use

With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information with an entity that maintains such information.

Privacy Rule

HIPAA Privacy Rule

The Privacy Rule is designed to assure that individuals' PHI is protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the publics' health and well being.

The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.

HIPAA Privacy Rule

Health Plans, Health Care Providers, Health Care Clearinghouses, and Business Associates are covered by the Privacy Rule.

All "*individually identifiable health information"* held or transmitted by a Covered Entity or its Business Associate, in any form or media -- electronic, paper, or oral is considered "*protected health information (PHI)."*

Protected Health Information (PHI)

The 18 Identifiers defined by HIPAA are:

- ✓ Name
- ✓ Postal Address
- ✓ All elements of dates except year
- ✓ Telephone Number
- ✓ Fax Number
- ✓ Email address
- ✓ URL address
- ✓ IP address
- ✓ Social Security Number
- ✓ Account Numbers
- ✓ License Numbers future
- ✓ Medical record number
- ✓ Health plan beneficiary #
- ✓ Devices identifiers and serial numbers
- ✓ Vehicle identifiers and serial numbers
- ✓ Biometric identifiers (finger and voice prints)
- ✓ Full face photos and other comparable images
- ✓ Any other unique identifying number, code, or characteristic

HIPAA Privacy Rule

Computer Practices

- Never share your computer passwords.
- Do not allow someone else to login to your computer using their passwords.
- Turn computer screens away from public view when possible. Implement screen savers when the monitor cannot be turned from view.
- Secure your computer when leaving your work area.

Enforcing the Final Rule

- **HIPAA Criminal Penalties**
  - $50,000 -- $1,500,000 fines
  - Imprisonment up to 10 years
- **HIPAA Civil Penalties**
  - $100 - $25,000 / year fines
  - More fines if multiple year violations
- **State of South Dakota corrective / disciplinary actions:**
  - Up to and including loss of privileges and termination of employment

How to Report Privacy Breaches

Immediately report any known or suspected privacy incidents or breaches (such as paper, conversations, suspected unauthorized or inappropriate access or use of PHI) to the agencies service director.

Confidentiality Agreement

Confidentiality Agreement...

At the end of this HIPAA general education, employees of certain agencies may be asked to sign a confidentiality agreement. By signing you agree to:

- Use confidential information only in performing your duties
- Dispose of protected health information properly
- Follow any agency policies and procedures

Privacy Rule Provisions

Protected Health Information (PHI) may be used or disclosed...

- For Payment of health care services received by consumers.
- For Treatment and to provide, coordinate , or manage consumer's health care and related services.
- For Health Plan Administration as necessary to administer and manage activities related to proving health care coverage.
- To Provide You Information on Health Related Programs or Products such as medical treatments and programs or health-related products and services.
- For Reminders about benefits or care, such as appointment reminders.

PHI may be used and disclosed under limited circumstances...

- As Required for Law such as Judicial or Administrative proceedings, or Law Enforcement purposes such as subpoena, search warrant, to locate a missing person, or report a crime.
- To Persons Involved With Care such as a family member in the event of an emergency.
- For Public Health Activities such as reporting or prevention of disease outbreaks.
- For Reporting Abuse, Neglect or Domestic Violence to government authorities that are authorized to receive and investigate reports.
- For Health Oversight Activities such as licensure, governmental audits, and fraud and abuse investigations.
- To Avoid a Serious Threat to Health or Safety such as disclosing information in the event of an emergency or natural disaster.

PHI may be used and disclosed under limited circumstances …

- For Specialized Government Functions such as military and veterans activities, national security and intelligence activities.
- For Workers' Compensation to the extent necessary to comply with state workers' compensation laws that govern job-related injuries or illness.
- For Research Purposes such as research related of certain treatments or the prevention of disease or disability.
- To Provide Information Regarding Decedents such as a coroner or medical examiner to identify a deceased person.
- For Organ Procurement, banking or transplantation of organs, eyes or tissue to facilitate donation and transplantation.

PHI may be used and disclosed under limited circumstances …

- To Correctional Institutional or Law Enforcement Officials for an inmate, and if necessary (1) for institution to provide health care to inmate; (2) to protect health and safety of inmates and others; or (3) for the safety and security of the correctional institution.
- To Business Associates that perform necessary functions or services on behalf of the covered entity. Business Associates are required, under contract, to protect the privacy of all PHI.
- For Data Breach Notification such as contact information to provide legally-required notices of unauthorized acquisition, access, or disclosure of health information.

Additional Restrictions on Use and Disclosure

Federal laws require special privacy protections of certain "highly confidential information", such as:

- HIV / AIDS;
- Mental Health, including psychotherapy notes;
- Genetic Tests / Information;
- Alcohol and Drug Abuse;
- Sexually Transmitted Diseases and Reproductive Health Information;
- Child or Adult Abuse or Neglect; and
- All PHI for use in marketing or sale, unless provided with an authorization of such use and disclosure.

Privacy Rule -- Consumer Rights

Individual Rights with respect to health information include...

- Access to health information such as claims, case or medical management records and a summary of health information.
- Disclosure Accounting of certain information made during the 6 years prior to the request.
- Restriction of uses and disclosures of health information for treatment, payment, health operations and health care for which an individual has paid out-of-pocket in full.

Individual Rights with respect to health information include…

- Confidential Communication such as receiving confidential communications in a different manner or at a different place.
- Amendment of health information if incomplete or inaccurate.
- Electronic Notice of health information.
- Filing a Complaint with the Secretary of the U.S. Department of Health and Human Services.

Security Rule

HIPAA Security Rule

- The Security Rule or the *Security Standards for the Protection of Electronic Protected Health Information* established a national set of security standards for protecting e-PHI. These standards are designed to protect the privacy of individuals' health information while allowing new technology to improve the quality and efficiency of health care.

- The Rule is designed to be flexible and scalable for a covered entity's size, organizational structure, and risks to consumers' e-PHI.

HIPAA Security Rule

- Health Plans, Health Care Providers, Health Care Clearinghouses, and Business Associates who transmit e-PHI are covered by the Security Rule.

- All “individually identifiable health information” held or transmitted by a Covered Entity or its Business Associate, in any form or media -- electronic, paper, or oral is considered “protected health information (PHI).”

HIPAA Security Rule
General Rules

To protect e-PHI, Covered Entities must maintain reasonable and appropriate

- Administrative Safeguards,
- Physical Safeguards, and
- Technical Safeguards

HIPAA Security Rule
General Rules

Covered Entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

HIPAA Security Rule
Administrative Safeguards

- Security Management Process –

  A Covered Entity must identify and analyze potential risks to e-PHI and implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

- Security Personnel –

  A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

- Information Access Management --

  A Covered Entity is required to implement policies and procedures for authorizing access to e-PHI, known as role-based access.

HIPAA Security Rule
Administrative Safeguards

- Workforce Training and Management –

  A Covered Entity must

  1) Provide for appropriate authorization and supervision of workforce members working with e-PHI,
  2) Train all workforce members regarding its security policies and procedures, and
  3) Have and apply appropriate sanctions against workforce members who violate its policies and procedures.

- Evaluation –

  A Covered Entity must perform a periodic assessment of its security policies and procedures.

HIPAA Security Rule
Physical Safeguards

- Facility Access and Control –

  A Covered Entity must limit physical access to its facilities while ensuring that authorized access is allowed.

- Workstation and Device Security –

  A Covered Entity must implement policies and procedures to specify proper use and access to workstations and e-media, and must have policies and procedures regarding transfer, removal, disposal, and re-use of e-media to ensure protection of e-PHI.

HIPAA Security Rule
Technical Safeguards

- Access Control –

  Allowing only authorized persons to access e-PHI

- Audit Controls –

  Implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems containing e-PHI

- Integrity Controls –

  Electronic measures to confirm that e-PHI has not been improperly altered or destroyed

- Transmission Security –

  Technical security measures guarding against unauthorized access to e-PHI being transmitted over an electronic network

Scenarios to Consider

Scenario #1

Your sister's close friend is receiving services from the department where you work. Your sister asks you to find out what you can about her friend's case. Should you look up the friend's medical information to give to your sister?

NO *– Even with the best of intentions, you do not have the right to access a friend's PHI. You should not seek out PHI unless needed to do your job. When you happen to hear confidential information, do not repeat it to anyone.*

Scenario #2

You are walking by a trashcan and notice a pile of photocopied records containing PHI has been laid on top of the trash. Should you shred the records?

NO *-- Gather the records and take them to your supervisor. He or she will report it to the department Privacy / Compliance Officer. The incident be will investigated.*

Scenario #3

You have seen the scheduled appointments for today in your department. You see the name of a close friend. Should you stop by to say hello?

No *--* *You should not stop by unless your job responsibilities require it.*

Scenario #4

A co-worker is having trouble logging in to the department's information system. They ask for your User ID and Password so they can try them. Should you share that information with them?

NO *– Under HIPAA standards, both the Privacy Rule and Security Rule require you to protect your User IDs and Passwords. Also, you should logout of programs that access PHI when not in use.*

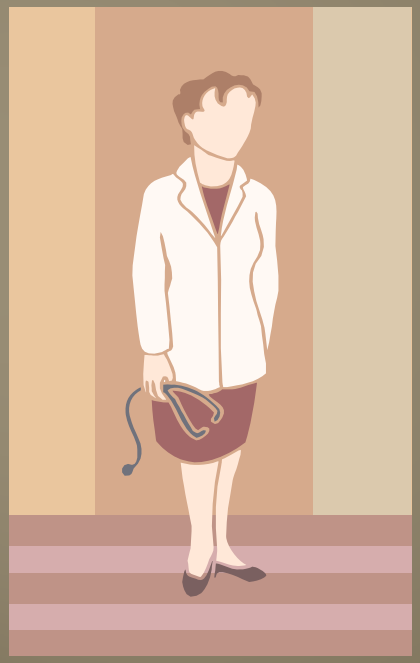
Test Your Knowledge

Question #1

When are you free to repeat protected health information that you hear while on the job?

a. After you no longer work for the department
b. After the consumer dies
c. Only if you know the consumer won't mind
d. Only when necessary to do your job

Answer



d.

You are allowed to release PHI that you learn while at work, only when necessary to perform your job.

Question #2

You see an open recycling bin full of paper. You can see names, addresses, and diagnoses on them. What should you do?

a. Nothing
b. Show it to your supervisor or your department's Privacy / Compliance Officer so the incident can be investigated
c. Read the report and try to figure out who disposed of it improperly
d. None of the above

Answer

b.

Your supervisor or department Privacy / Compliance Officer should be notified so that the incident can be investigated. All documents containing PHI must be disposed of properly.

Question #3

What question should you ask yourself before looking at a consumer's information?

a. Would the consumer mind if I looked at this?
b. Do I need to know this to do my job?
c. Can anyone see what I'm doing?
d. All of the above

Answer

b.

While performing your job duties, you may need access to a consumer's PHI. You should remember that you only need the information related to performance of that duty.

Question #4

Which of the following is NOT a common practice to protect the confidentiality of consumer's information?

a. Keeping computers logged out of the information system when not in use
b. Storing paper records in locked file cabinets or rooms
c. Throwing paper containing PHI in the trash can
d. Pointing computer screens away from the public when possible

Answer

c.

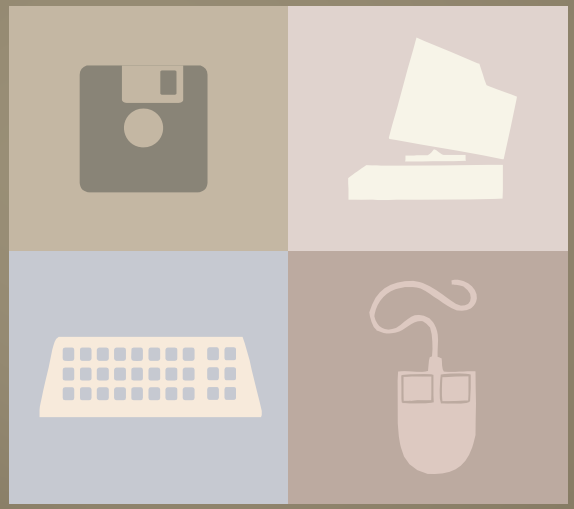
Documents containing PHI should be disposed of properly, by shredding or placing in a secure area for recycling.

Question #5

Under what circumstances is it acceptable to logon to a co-worker's computer?

a. When your co-worker forgets his/her password
b. When sending a birthday greeting
c. When you know you can trust the person to use it wisely
d. Never

Answer



d.

Remember that if someone uses your computer or password you may be held responsible for inappropriate use by the other party.

Question #6

Which of the following is considered protected health information under HIPAA?

a. The consumer's address
b. The consumer's medical record number
c. The consumer's phone number
d. All of the above

Answer

d.

These items and others are considered PHI. Check with your supervisor or your department's Privacy / Compliance Officer for more information.

Question #7

Which of the following types of information does HIPAA's Privacy Rule and Security Rule protect?

a. Consumer information in electronic form
b. Consumer information communicated orally
c. Consumer information in paper form
d. All of the above

Answer

d.

The HIPAA Privacy Rule and Security Rule protect information used or disclosed in electronic, oral and written format.

Question #9

What should you do if a consumer complains about their rights being violated under HIPAA?

a. Notify your department's Privacy / Compliance Official who is responsible for handling complaints
b. Ask the program participant not tell anyone
c. Nothing – It's not your job to handle complaints
d. None of the above

Answer

a.

The Privacy / Compliance Officer is responsible for investigating any complaint filed by a consumer.

Question #10

What type of rule is HIPAA?

a. A state law imposed on clinics only
b. A federal law imposed on all health plans, health care providers, and health care clearinghouses
c. A guide set forth by the South Dakota Department of Health
d. A local law

Answer

b.

HIPAA is a federal law that all health plans, health care providers, and health care clearinghouses must follow. The HIPAA regulation is published in the Federal Register.

Thank You

Instructions: To close the HIPAA Training Module, click Esc on your computer. Then, complete the following certificate and provide a copy to your service director.

Course Completion Certificate

SOUTH DAKOTA DEPARTMENT OF HEALTH

Certificate of Completion

This certificate verifies that

_____

Name

has successfully completed the
Health Insurance Portability and Accountability Act (HIPAA)
training program approved through the SD Department of Health.

Please print, sign, and date this certificate and make available to your service director. This will need to remain on file.

_____ _____

Service Director *Date of Completion*