



HIPAA and Information Security Basics for the DOH Workforce



*Health Insurance Portability
and Accountability Act (HIPAA)*



Training Objectives

1. Understand the purpose of HIPAA and the Privacy Rule
2. Understand why DOH must comply.
3. Understand the term “protected health information”
4. Understand the rules for use and disclosure of protected health information
5. Understand the Notice of Privacy Practices and clients’ rights.
6. Understand that the DOH may still share protected health information with its business associates while following HIPAA requirements.
7. Know where to find DOH privacy policies and procedures.
8. Know who the Privacy Officers and the DOH Privacy Complaint Officer are.





Intent of Training

- This training is intended for new DOH employees, contracted providers, and volunteers.
- This training is an overview of the HIPAA regulations and the DOH Information Security and Privacy policies. It does not cover all policies and procedures that the DOH workforce is to abide by.
- It is advised that all DOH employees, contracted providers, and volunteers review the HIPAA regulations and DOH Information Security and Privacy policies to get a complete understanding of what he/she is responsible for.



Course Outline

- Overview of the Federal HIPAA legislation
- The HIPAA *Privacy Rule*
- Protecting Client Information
- Client Rights
- DOH Information Security and Privacy Policy and Procedures





What is *HIPAA*?



What is HIPAA?

Health Insurance Portability and Accountability Act

- The purpose of HIPAA is to improve the efficiency and effectiveness of the country's health care system.
 - By establishing standards for electronic transmission of health information.
 - By establishing standards to protect the privacy of individuals' medical records and other protected health information.
 - By ensuring the security of health care information.



HIPAA Privacy



- HIPAA Privacy Regulations establish national standards for protecting the privacy of health information.
 - They impose new restrictions on the use and disclosure of protected health information.
 - They give patients greater access to and protection of their medical records and more control over how they are used.



DOH must comply with HIPAA

- Covered entities must comply with HIPAA.
 - A covered entity is a:
 - Health Plan
 - Health Care Clearinghouse
 - Health Care Provider
- Many activities we carry out closely match the HIPAA definition of a Health Care Provider, especially those involving Medicare and Medicaid.



What does this have to do with me?

- 
- Client records
 - Disease reporting
 - Registries
 - Identifiable client information

family planning

medical records
sexually transmitted diseases
AIDS/HIV

tuberculosis
bioterrorism

vital statistics

Contracted client services

public health reporting

chronic disease management

healthy start

HIPAA rules apply to a significant part of the agency and to those unit employees.



What does the HIPAA *Privacy Rule* Require?



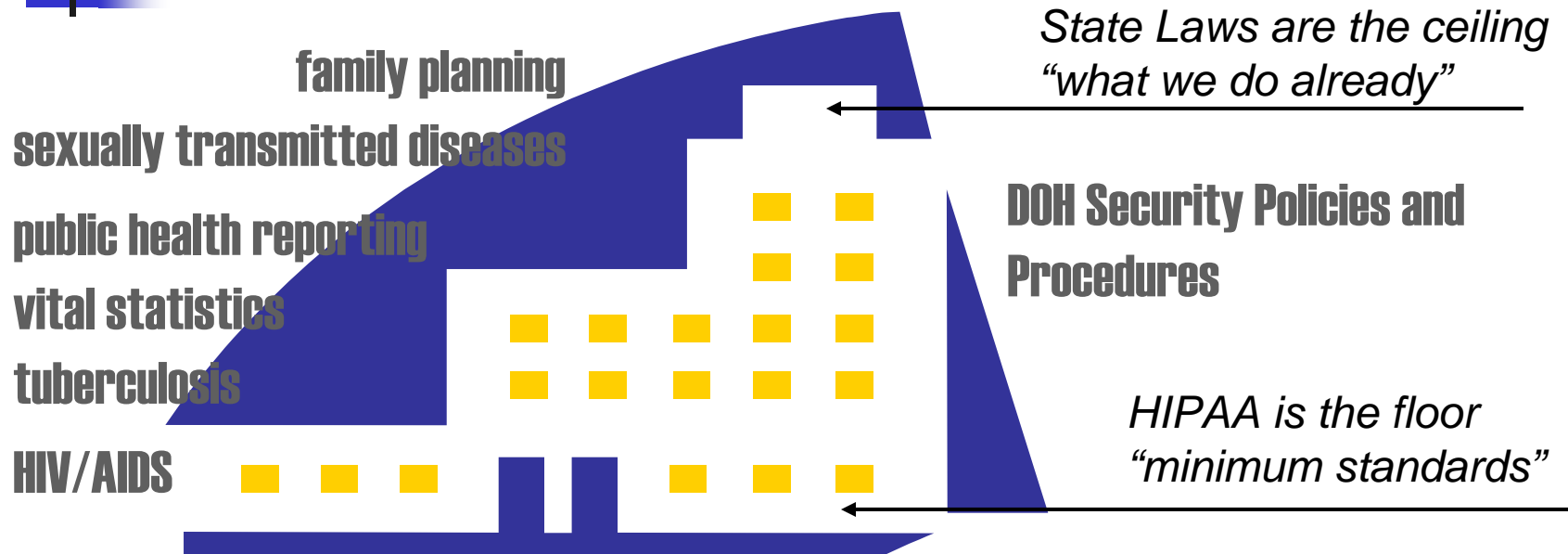
The HIPAA *Privacy Rule*

- Establishes safeguards to protect the privacy of health care information
- Sets boundaries on the use and release of health records
- Holds people accountable if they violate patient rights (civil and criminal penalties)





HIPAA rules and Florida law



In many instances, Florida laws are more stringent than HIPAA requirements. DOH staff have been protecting health information for many years and already have many safeguards and procedures in place.



DOH Responsibilities



- Notify patients about their privacy rights
- Adopt and implement privacy procedures across the agency
- Train employees on privacy procedures
- Ensure that business associates protect our patients' information
- Designate an agency Privacy Officer, a Privacy Complaint Officer and Local Privacy Officers
- Establish a Complaint Procedure



What is a *Business Associate*?

- Individuals or companies hired to do work for a covered entity that requires the use or disclosure of protected information.
 - Examples:
 - Biomedical waste transport
 - Transcription firms
 - Case Management





What is

Protected Health Information?



Protected Health Information (PHI)



- Individually identifiable health information
- Transmitted or maintained in any electronic, written, or spoken format.
 - For example, e-mail, fax, on-line databases, voice mail, video/audio recordings, or conversations.
- HIPAA calls protected health information *PHI*.



What is protected health information?



- Helen Hippo
- Lives in Orlando, Florida
- Suffers from hypertension
- Receives prenatal care and care coordination services
- Participates in WIC program





The following are examples of identifiers:

- Names
- Addresses
- Dates directly related to an individual such as birth date, admission date, discharge date, and date of death
- Telephone numbers
- 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
- Biometric identifiers, including fingerprints and voice prints
- Full face photographic images .

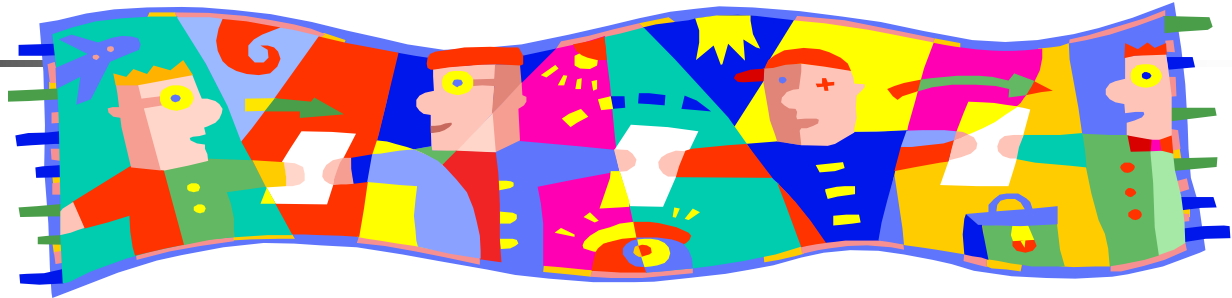


Protected Health Information (PHI) Use and Disclosure

- The *Privacy Rule* prohibits use or disclosure of protected health information unless:
 - It is used to provide treatment, payment, or health care operations, or
 - It's use is authorized by the client, or
 - Not sharing the information would present a risk to public health or safety. (example: Disease Reporting as required by statute, bioterrorism activities).



Incidental Uses and Disclosures



- Incidental uses and disclosures occur as a result of an initial use or disclosure that is permitted.
- These are allowable as long as *reasonable safeguards* are taken and the sharing of protected health information is *limited to the minimum necessary to do the job*.
 - *An incidental use is a re-disclosure of health information*



Use *Reasonable Safeguards*

- Reasonable Safeguards are the actions the Department takes to ensure that protected health information remains private.
- When there is incidental use or disclosure of health information, use these *reasonable safeguards*:
 - Access is limited
 - Authorization is obtained prior to sharing (when applicable)
 - Client information is secure.



Reasonable Safeguard Examples:

The DOH Security Policy specifies precautions that should be taken to assure information privacy and security.

- Speak quietly when discussing a client's condition with family members or others.
- Avoid using client names in elevators and hallways.
- Secure documents in locked offices and cabinets.
- Do not leave unauthorized persons unattended in restricted areas.
- Use passwords and other security measures on computers.





Minimum Necessary Standard

- The minimum necessary means that the department will develop policies and procedures that limit the sharing of protected health information to the minimum necessary to do the job.

The policy must:

- Limit who has access to protected health information.
- Specify the conditions under which this information can be accessed.





What are the clients' rights?



Clients have the right to:

- Receive a written notice of the Department's privacy practices.
- Require their authorization for the release of information.
- Request restrictions on the use of their PHI.
- Inspect and copy their PHI – as documented by the Department.
- Request that improper uses are corrected.
- Obtain a report of disclosures of their PHI.
- File a grievance or complaint.

The DOH's Information Security and Privacy Policy

- DOH Information Security and Privacy policies are to be followed when more stringent than HIPAA.
- Establishes a uniform process for implementing and disseminating the privacy standards required by HIPAA regulations within DOH.
 - Privacy Operating Procedures
 - Notice of Privacy Practice and updated DOH forms containing HIPAA privacy language
 - Complaint/Grievance procedures for clients





DOH Privacy Policy



- Employees, contracted providers/business associates and volunteers will be trained about the privacy policy.
- Record of this training will be maintained in the personnel file; or with contract manager when applicable.
- The policy is accessible on the web and available to all employees.

Violation of this policy will result in disciplinary action and may also have criminal and civil penalties.



Notice of Privacy Practices

- Written for our clients, parents or guardians of clients to explain:
 - The Department's HIPAA related duties
 - Reasons the Department will use/share protected information
 - Client rights
 - How to file a complaint or grievance

Notice of Privacy Practices

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

PLEASE READ IT CAREFULLY





Notice of Privacy Practices

- A poster about privacy rights will be visibly posted at each facility or health center.
- All new clients will be provided with a copy of the *Notice of Privacy Practice* at time of initial contact with the Department.
- All existing clients will be provided with the *Notice of Privacy Practice* at their first visit starting April 14, 2003.



Complaint /Grievance Procedure

Client believes rights under HIPAA
may have been violated



Patient files a written complaint with the
local Privacy Officer



Local Privacy Officer coordinates investigation
with DOH Privacy Complaint Officer
(Inspector General)



If issue not resolved to patient satisfaction, he or
she can file a complaint or grievance with the
Department of Health and Human Services
Office of Civil Rights or the DOH Privacy
Complaint Officer in Tallahassee.





The Department's Privacy Officer

Office of the General Counsel

2585 Merchants Row Boulevard
Tallahassee, FL 32399
850-245-4005





The DOH's Privacy Complaint Officer

- Office of the Inspector General

4052 Bald Cypress Way, Bin A03
Tallahassee, FL 32399
850-245-4141

- Clients who have feel that DOH has not followed the HIPAA privacy rule should send written complaints for investigation.





HIPAA Information Resources

- DOH Policies and Procedures

are available electronically on the DOH web site:

http://www.doh.state.fl.us/planning_eval/HIPAA/index.html

http://dohiws.doh.state.fl.us/Divisions/IRM/Policies/Security/table_of_contents.htm

- US Dept. Of Health and Human Services:

<http://www.hhs.gov/ocr/privacy/index.html>

The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH*
Information Security and Privacy Policies





DOH must:

- Safeguard the privacy of protected health information, which includes past, present, or future
 - health conditions,
 - provision of health care,
 - payment for health care.
- Provide notice of the Department's privacy practices.
- Explain how, when, and why we may disclose or use protected health information.
- Monitor compliance with the information security and privacy policies, protocols, and procedures.

The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH Information Security and Privacy Policies*

General Rules:



- Use and disclose information only within the limits of DOH policy.
- Document disclosures of client information in the record.
- Allow clients access to their health information and allow requests to amend health information.
- Keep client records secured in a reliable locking system within a restricted area, and not leaving confidential information unattended.
- Only send/take just enough confidential information to satisfy the request/task.
- Confidential information being discussed by phone, must be done so in areas where the conversation cannot be overheard.
- Cellular phones (including the Blackberry) are not considered to be secure.

The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH Information Security and Privacy Policies*

General Rules:



- All DOH employees, contracted providers and volunteers must have access to DOH Information and Security policies.
- Individual medical information maintained in a public health disaster, emergency, communicable disease surveillance, or epidemiology investigations are exempt from HIPAA.
- Use encryption when sending confidential information electronically over a public transport medium or the transport medium is not owned or managed by the department. Keeping in mind most state communications to or from state officials regarding state business are public records.
- Double enveloping is required when mailing confidential or sensitive information.
- Report all breeches of client confidentiality to your supervisor, local privacy officer, or Inspector General.

The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH Information Security and Privacy Policies*



Allowable uses of protected health information

- DOH may use protected health information without the client's written authorization for the following reasons:
 - For treatment
 - To obtain payment
 - For department/healthcare operations



The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH Information Security and Privacy Policies*



Exceptions to the written authorization rule

- The Department can use or disclose protected health information without written authorization for the following reasons:
 - The law requires disclosure
 - For public health activities
 - For health oversight activities
 - To avert threats to health or safety
 - For research purposes with IRB approval



Exceptions to the written authorization rule

- Law enforcement
 - Relating to decedents
 - Investigation of a crime
 - Medical examiners / funeral directors
- Subpoenaed Medical Records
 - General patient medical information records (excluding public health investigatory records, HIV test results, substance abuse service provider client record and WIC records) may be disclosed under the authority of a subpoena, but only after the patient or patient's authorized representative has had an opportunity to object and has not.

The *BOTTOM LINE* on Implementing *HIPAA* and the *DOH Information Security and Privacy Policies*



Test your knowledge:

1. Who must follow HIPAA privacy requirements?
 - A. All DOH staff and volunteers
 - B. Staff who work with clients
 - C. All staff and volunteers who work with protected health information

2. The privacy rule...
 - A. replaces Florida's existing confidentiality laws
 - B. protects individually identifiable information
 - C. requires a court order for records release



Test your knowledge:

3. Allowable use of PHI is for reasons of treatment, payment or operations.
 - A. True
 - B. False

4. What does protected health information include?
 - A. Any information that can link a specific person with a health condition
 - B. Written, spoken or electronic communication about an individual's health information
 - C. Both



Test your knowledge:

5. The DOH may no longer share information about clients with business associates.
 - A. True
 - B. False

6. All clients must be provided with written notice of the Department's privacy practices.
 - A. True
 - B. False



Test your knowledge:

7. Incidental uses or disclosures of PHI are allowed if:
 - A. The client has provided written consent
 - B. The request comes from headquarters
 - C. Reasonable safeguards are in place

8. You must obtain patient agreement to use or disclose PHI for public health activities.
 - A. True
 - B. False



Test your knowledge:

9. Clients have the right to request a history of non-routine disclosures that have been made.
 - A. True
 - B. False

10. Clients may formally complain to the Department of Health or to the Department of Health and Human Services if they feel their privacy has been violated.
 - A. True
 - B. False



Check your answers:

1. C

2. B

3. A

4. C

5. B

6. A

7. C

8. B

9. A

10. A



HIPAA and DOH Information Security and Privacy Training

Employee Name : _____ Date: _____
 Print Name

This document functions as confirmation of successful completion of the Department of Health's HIPAA and Information Security and Privacy Training program and the individual named above has completed said training.

Signature of Employee: _____ Date: _____

Attested to by: _____ Date: _____
 Supervisor/Privacy Officer/Contract Manager





The End

