



**Louisiana Department of Health and Hospitals
Basic HIPAA Privacy Training: Policies and Procedures**

What Is HIPAA?

- **HIPAA (pronounced hippa) is a federal law.**
- **It's a set of rules and regulations that affect the health care industry.**
- **They focus on the privacy and security of health care information.**
- **We in the Department of Health and Hospitals (DHH) must comply, as HIPAA covers:**
 - **Health Plans**
 - **Health Care Providers**



What Does The Privacy Rule Say?

- Sets rules for how private information can be used.
- Keeps clients/participants more informed.
- Limits access by others.
- Requires client/participant permission.
- Allows access by clients/participants.
- Requires that rules be followed.
- Increases safeguards.
- Enforces penalties.
- Requires training for everyone in DHH.



Individually Identifiable Health Information

- **Information about health care or payment for health care, such as:**
 - **Why a person is visiting the clinic or center;**
 - **The type of treatment a person is receiving; or**
 - **The fact that a person is receiving Medicaid.**

 - **That:**
 - **Identifies the person; or**
 - **Could possibly identify the person.**

- **Examples of such information include a client/participant's name, address, social security number, medical record number, or photograph.**

Protected Health Information (PHI)

- **PHI is all individually identifiable health information in any form:**

- **Paper**
- **Verbal**
- **Electronic**



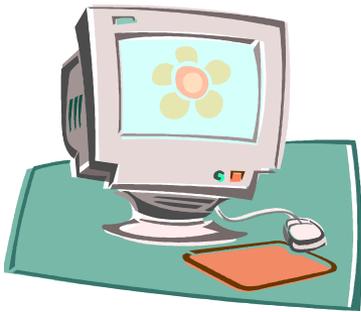
- **Exceptions:**

- **Employment records (including employees' medical information).**
- **Certain education records.**

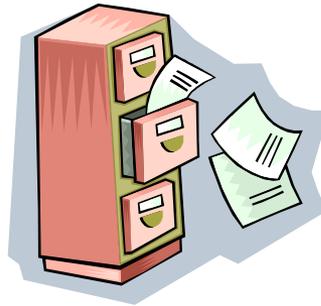


PHI

- Protected Health Information can be stored in/on:



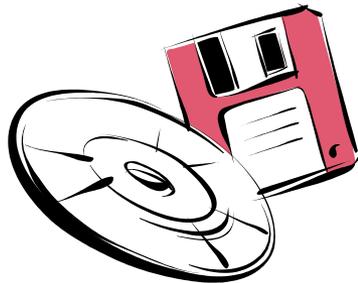
Computers



File Cabinets



Desks/Offices



Disks/CDs



Iphones/IPAD



Privacy Notice

- **HIPAA requires DHH to write a Privacy Notice.**
- **The DHH Notice of Privacy Practices (NPP) tells how we can use or disclose PHI about our clients and participants.**
- **Beginning April 14, 2003, we must give a Privacy Notice to every client who comes to our offices to ask about or receive services.**



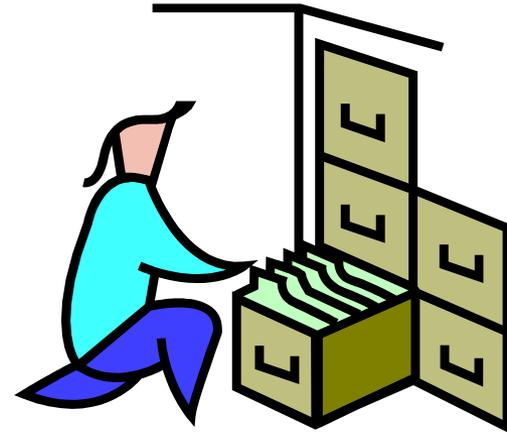
“Use” and “Disclose”

- You *use* Protected Health Information within DHH.
- You *disclose* PHI to persons or organizations outside DHH.



Minimum Necessary Requirements

- You are only allowed access to the minimum amount of PHI necessary for you to perform your job duties.



- You must only disclose the minimum amount of PHI necessary to satisfy a request.
- You must only request the minimum amount of PHI you need at the time.

Minimum Necessary – Not Applicable

- **The minimum necessary rule does not apply to:**
 - **Disclosures to, or requests by, a health care provider for treatment;**
 - **Uses or disclosures made to the client/participant;**
 - **Uses or disclosures that the client authorized;**
 - **Disclosure made to the Secretary of HHS; and**
 - **Disclosures required by law.**



Verification Requirements

- **Prior to disclosing PHI, you must:**
 - **Verify the identity of the person requesting PHI and the authority of that person to have access to PHI; and**
 - **When required, get some kind of proof from the person making the request.**



■ Treatment



■ Payment



■ Health Care Operations (Examples):

- Quality Assessment and Improvement;
- Medical Review and Auditing;
- Planning and Budget



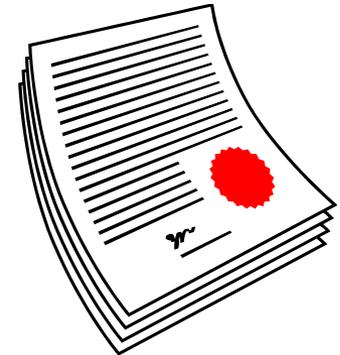
Permission To Use or Disclose PHI?

- **For Abuse Reports and Investigations.**
 - DHH is required by law to receive and investigate reports of abuse, neglect or exploitation.
- **Generally, however, you do need specific, written authorization from the client/participant before you can use or disclose his or her PHI for other reasons (unless specifically permitted by the Privacy Rule).**



Administrative Requirements

- You must follow DHH's HIPAA-compliant **policies and procedures** unless your office already has rules about privacy or confidentiality that are more strict than HIPAA.
- DHH's nine privacy policies are in the Policy Manual, which is posted on SharePoint at <http://dhhnet/departments/omf>.



Administrative Requirements (continued)

- You must participate in privacy **training** annually on DHH's policies and procedures for using and disclosing PHI.
- *You're getting some of that training right now!*



Administrative Requirements (continued)

- You must follow DHH's **safeguards** designed to protect the privacy of clients/participants' PHI.
 - **Technical**
 - Restricted access to computer databases
 - Periodic password changes
 - Restrictions on emails
 - **Physical**
 - Security of records and files
 - Shredding and other disposal methods



Administrative Requirements (continued)

- **Staff who violate the DHH's policies and procedures regarding PHI are subject to disciplinary action up to and including dismissal.**
- **You could even be fined and jailed if you break the law.**



If You See A Problem...

- **If you see or hear about someone who is not following DHH's policies and procedures, you should tell your supervisor.**



- **All reports should be investigated.**



Prohibition on Retaliatory Acts

- **DHH is bound by law to protect a workforce member from harassment or retaliatory actions if he or she reports a suspected privacy violation.**



Crime Victims

- **You are allowed to disclose PHI to law enforcement without the client/participant's authorization when:**
 - **The PHI disclosed is about the person suspected of a criminal act; and**
 - **The PHI disclosed is limited to information relevant to identifying the suspect and the nature of any injury.**



Scenario 1 – Question

- **You work for the cleaning staff and you tell a co-worker about a bill you saw while cleaning an office in which a client, Mr. Smith, received chemotherapy.**
- **Question #1: Is the information contained on the bill considered PHI?**
- **Question #2: Can you discuss what you saw?**
- **Question #3: Could you be liable for improper use and disclosure of PHI?**



Scenario 1

- **Take a few moments to think about your answer(s).**



Scenario 1 – Answer

- **Question #1: Is the information contained on the bill considered PHI?**
 - **Answer: Yes. The client's name alone is Protected Health Information.**

- **Question #2: Can you discuss what you saw?**
 - **Answer: No. Your job duties do not require that you have access to any billing information for you to do your work.**

- **Question #3: Could you be guilty of improper use and disclosure of PHI?**
 - **Answer: Yes. The fact that you are discussing an individual's bill is against the Minimum Necessary policy. You could be liable for misuse of PHI.**



Scenario 2 – Question

- **After printing a report that contains social security numbers, you realize there is a mistake in the report and you need to print a new one. You throw the old report in the trash.**
 - **Question #1: Is the information contained on the old report protected under HIPAA?**
 - **Question #2: What should be done with the old report?**
 - a. **Put in bin for office coordinator to recycle**
 - b. **Destroy the old report according to office procedures**
 - c. **Throw in trash for DCI to pick up**



Scenario 2

- **Take a few moments to think about your answer.**



Scenario 2 – Answer

- **Question #1: Is the information contained on the old report protected under HIPAA?**
 - **Answer: Yes. Social security numbers can be used to identify individual clients.**

- **Question #2: What should be done with the old report?**
 - **Answer: b. destroy the old report according to your office procedures.**



Scenario 3 – Question

- **As you are opening and sorting mail to be delivered to various departments within your organization, you notice that a complaint regarding the payment of a claim in the amount of \$1,000 has come in from the person who lives next door to you.**
 - **Question #1: Is the information you see protected under HIPAA?**
 - **Question #2: Do you have a right to read the complaint?**
 - **Question #3: When you get home, can you tell your spouse about the complaint?**



Scenario 3

- **Take a few moments to think about your answer.**



Scenario 3 – Answer

- **Question #1: Is the information you see protected under the Privacy Rule?**
 - **Answer: Yes. PHI includes financial information related to payment for health care services.**
- **Question #2: Do you have a right to read the complaint?**
 - **Answer: No. Your job duties do not require that you read the actual complaint, but only that you know that such a document is a complaint so that it is routed to the appropriate department.**
- **Question #3: When you get home, can you tell your spouse about the complaint?**
 - **Answer: No. The person filing the complaint has a right to privacy regarding his or her PHI.**



Scenario 4 – Question

- **You are asked to e-mail PHI to a co-worker within DHH. Later, you are asked by the same co-worker to fax PHI to someone at another health plan.**
 - **Question #1: What safeguards should be in place to protect the privacy of the PHI being sent via e-mail?**

 - **Question #2: What safeguards should be in place to protect the privacy of the PHI being sent via fax?**



Scenario 4

- **Take a few moments to think about your answer(s).**



Scenario 4 - Answer

- **Question #1: What safeguards should be in place to protect the privacy of the PHI being sent via e-mail?**
 - **PHI should never be included in an e-mail sent outside DHH.**
 - **If you think you have good reason to not follow the two rules above, see your supervisor.**



Scenario 4 – Answer

- **Question #2: What safeguards should be in place to protect the privacy of the PHI being sent via fax?**
 - **Answer: Ensure that the out-going fax number is correct and follow-up with the recipient to ensure that the fax was received. For incoming faxes, ensure that the fax machine is located in a secure area where there is no public access.**
 - **The fax should also contain a confidentiality statement indicating that the information contained within the fax is private.**
 - **If necessary, you should verify the identity of the person requesting the PHI and, if appropriate, obtain documentation confirming the recipient's authority to request PHI.**
 - **All information contained within the fax should meet the Minimum Necessary test.**



Scenario 5 – Question

- **You and a co-worker are in your office with the door open discussing the cost of a client's claim (for a report you both are working on) when someone else walks in and overhears you mention the client's name and that his medical costs were \$10,000.**
 - **Question #1: Is what the person heard considered PHI?**
 - **Question #2: Are you allowed to discuss PHI around others?**



Scenario 5

- **Take a few moments to think about your answer(s).**



Scenario 5 – Answer

- **Question #1: Is what the person heard PHI?**
 - **Answer: Yes. A client's name overheard is still protected health information under the Privacy Rule.**

- **Question #2: Are you allowed to discuss PHI around others?**
 - **Answer: Yes. The Privacy Rule allows for “incidental disclosures” of PHI without penalty as long as reasonable efforts are made to keep others from overhearing a conversation. For example, talking quietly while in public areas.**
 - **The best approach is to only discuss PHI within a private setting where no one will overhear your conversation. In this scenario, the best approach would have been to close the door to your office so that others wouldn't overhear your conversation.**



Scenario 6 – Question

- **You work for the food service and are given a list of patients who need special menus due to their various conditions. You do not know their various conditions, but you do know their names and room numbers.**
 - **Question #1: Is the information you are given considered PHI?**

 - **Question #2: What can you do and not do with the information you are given?**
-



Scenario 6

- **Take a few moments to think about your answer(s).**



Scenario 6 – Answer

- **Question #1: Is the information you are given considered PHI?**
 - **Answer: Yes. Patient name is PHI under the Privacy Rule.**

- **Question #2: What can you do and not do with the information you are given?**
 - **Answer: You can use the information you are given to perform your job duties (i.e., prepare the appropriate meals). This use of PHI would fall under “treatment” and does not require obtaining permission from the patient.**
 - **You cannot use the patient name, his room number, or the fact that he is in the hospital for any other reason. Use of such information outside of “treatment” is against the Privacy Rule.**



Scenario 7 – Question

- **In a monthly summary report you normally review as part of your job duties, a copy of an individual's claim is attached to explain something in the report. The attachment contains the patient's name, address, and reason for seeking services. You recognize the patient's name as your neighbor, Jim. You didn't previously know he had been ill.**
- **Question: When you get home, can you go to Jim's house and ask him how he is doing?**



Scenario 7

- **Take a few moments to think about your answer.**



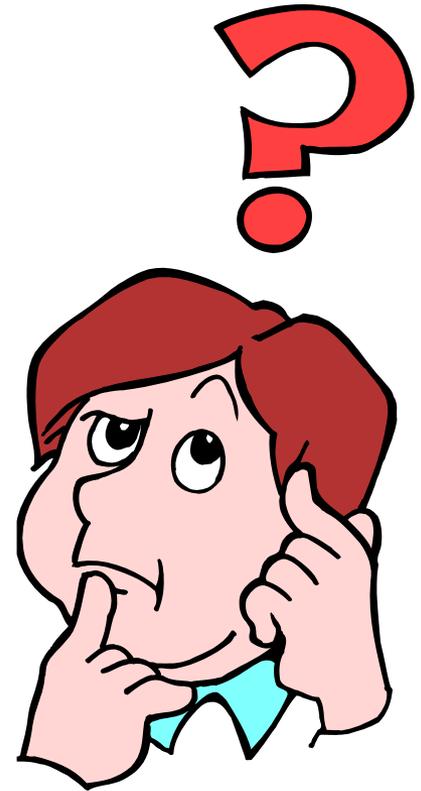
Scenario 7 – Answer

- **Question: When you get home, can you go to Jim's house and ask him how he is doing?**
- **Answer: No. You learned of his treatment as part of your job. Disclosure to him or anyone else regarding his illness (except for reasons of treatment, payment or DHH operations) is against the Privacy Rule. You could face disciplinary action.**



Remember...

- If you are unsure about how to proceed in a certain situation involving PHI, ask your supervisor.
- DHH has a Privacy Officer who serves as the final authority on questions raised through your chain of command.



Remember...

- Do not discuss any PHI you see or hear while performing your job with anyone unless necessary!



Remember...

- **There are significant penalties for misuse of PHI.**



You're Making HIPAA Happen . . .





DHH HIPAA PRIVACY TRAINING ACKNOWLEDGEMENT FORM

As a contract employee of the Department of Health and Hospitals (DHH), I,
_____ have reviewed and understand the DHH HIPAA Privacy Policies and Procedures. I am aware that violations of the policies and procedures subject me to disciplinary action up to and including dismissal. I agree to abide by the DHH HIPAA Privacy Guidelines.

Contract Employee Signature

Date