Confidentiality and HIPAA

Adapted from:
Louisiana Department of Health and Hospitals
Basic HIPAA Privacy Training: Policies and Procedures
PLEASE NOTE!

When you have completed this training, you will be directed to access the test via a link in the final slide.
OBJECTIVES

At the end of this session, the participants will be able to...

• Define and explain HIPAA
• Identify which information is governed by HIPAA
• Define Protected Health Information (PHI)
• Explain verification requirements
• Explain rules governing obtaining permission to disclose PHI
• Discuss the employee’s role if they are aware of a HIPAA violation
• Explain appropriate use of social media
Get It Right!

HOLD UP

IT'S HIPAA NOT HIPPA

memegenerator.net
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.
• Health care providers 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
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
Individually Identifiable Health Information

• Information about health care or payment for health care, such as:
  • Why a person is visiting the program or center;
  • Why you are visiting the person;
  • The type of treatment a person is receiving; or
  • The fact that a person is receiving Medicaid.
  • The fact that someone is receiving services.

• Anything 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.
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

What does “minimum necessary” mean?

After receiving consent from the client, you may supply...

- A summary of the case record, including most recent diagnosis
- A statement about participation in the program
- A general statement about progress or lack thereof
- Number of times the client was seen over a span of time
Disclosures

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; or
- Disclosures required by law.
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.

• The PHI disclosed is **limited to information relevant to identifying the suspect** and the nature of any injury.
General 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.

• When required, get some kind of proof from the person making the request.
THINGS TO THINK ABOUT

Situations that often lead to violations of confidentiality:

• Discussing work with family and friends
• Informal discussions with colleagues
  • Hallway, elevator, lunch break, grocery store
• Social gathering
  • Office parties, etc.
• Incoming phone calls
• Attentive non-employees working at agency (repairmen)
Scenario #1

You keep forgetting your password to log on to your facility's system, so you write it on a sticky note that you leave on your desk. Is this an acceptable practice?
No. You must not keep your password where others can access it easily. If someone finds your password and logs on to the facility's system as you, you can be held accountable for anything that happens as a result. If you have trouble coming up with a password you can remember, ask your information technology (IT) department or information security officer for help.
Violation Consequences

• Failure to comply with HIPAA is a violation of federal law.

• The HIPAA **Enforcement Rule** (codified at 45 CFR Part 160, Subparts C, D, and E) establishes procedures for the investigation of possible HIPAA violations and sets civil fines for infractions. Fines can be up to **$50,000 per violation per day**, so it can add up quickly and is not a joke.

• Violations can also carry criminal penalties, including fines and jail time, but these are not covered by HHS regulation.
• A breach of protected health information ("PHI") is defined as the acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.
NOTABLE SETTLEMENTS & PENALTIES

Cigna Health
February 2011 - Cigna Health was fined $4.3 million for failing to provide 41 patients copies of their medical records upon request and subsequently failing to cooperate with an investigation.

CVS Caremark Co.
February 2009 - CVS was fined $2.25 million for failing to implement adequate policies, procedures and training to safeguard patient information when they disposed of information, such as pill bottle labels.

Blue Cross Blue Shield of Tennessee
March 2012 - BCBST agreed to pay $1.5 million to settle potential violations after a report that 57 unencrypted computer hard drives containing protected health information of more than 1 million individuals had been stolen.

Mass General Hospital
February 2011 - Massachusetts General Physicians Organization, Inc. (Mass General) reached a $1 million settlement agreement for the loss of patient information on a subway.

Phoenix Cardiac Surgery
April 2012 - Phoenix Cardiac Surgery, a five-physician practice agreed to pay $100,000 over violations of HIPAA Privacy and Security rules.
If You See a Problem...

- If you see or hear about someone who is in violation of HIPAA requirements and procedures, you should tell your supervisor.
- All reports should be investigated.
- The HIPAA Breach Notification Rule (codified at 45 CFR §§ 164.400-414) requires healthcare organizations to provide notification after breaches of PHI. A “breach” is, basically, an impermissible use or disclosure of PHI, as detailed in the HIPAA Privacy Rule. Depending on the type of breach, notification might need to be made to the affected individuals, the media, or the HHS Secretary. HHS has further guidance available on the topic.
An employer is bound by law to protect a workforce member from harassment or retaliatory actions if he or she reports a suspected privacy violation.
Remember...

- If you are unsure about how to proceed in a certain situation involving PHI, ask your supervisor.
- Do **not** discuss any PHI you see or hear while performing your job with anyone unless necessary!
- There are significant penalties for misuse of PHI.
Scenario #2

A personal care attendant goes to church with his client and learns from documentation that the client has a terminal illness. He then calls other members of the church who put the information out on a prayer chain. Suddenly, several hundred people know about the person's illness. Is this an acceptable disclosure?
Pop Quiz

No. If you view client records for any nonbusiness reason, it is grounds for dismissal and possible legal consequences. Likewise, if you view the records for the right reasons but pass the information along to others who don't have a right to know, you also violate your organization's policy and the law.
Q: What should I do if a government agency or law enforcement person requests information about a client?

A: If working with law enforcement is not part of your responsibility, contact your supervisor. If it is your responsibility, provide only the minimum amount necessary to support the investigation after verification of the authority of the individual or organization making the request. Always consult your supervisor or HR if you are unsure what to do. The privacy rules are very specific in this area.
Q: What if I get a phone call looking for information, and the caller says he/she is the client? What should I do?

A: The caller must sign a consent for release of information in person.
Q: What if I get a request for case records from an attorney?

A: You should NOT give them all their records. After receiving consent from the client, you may supply a summary of the case record, including most recent diagnosis, a statement about participation in the program, a general statement about progress or lack thereof, and number of times the client was seen over a span of time. REMEMBER: Only disclose the minimum amount of PHI necessary to satisfy a request.
Q: What if there’s a court order for release of information?

A: You should NOT give them all their records. After receiving consent from the client, you may supply a summary of the case record, including most recent diagnosis, a statement about participation in the program, a general statement about progress or lack thereof, and number of times the client was seen over a span of time. REMEMBER: Only disclose the minimum amount of PHI necessary to satisfy a request.
Q: May I use texting and/or email to communicate with a client?
Q: I know that clients have a right to their PHI, but what about parents/guardians of incompetent clients?

A: If someone other than the client has the legal right to make healthcare decisions for the client, that person is the client’s personal representative and has the right to access the client’s PHI. However, if you have good reason to believe that informing the personal representative could result in harm to the client or others, then you do not have to disclose the PHI.
Q: As part of my job, I have access to a client’s PHI. How do I know which family and friends can be told this information?

A: Always ask the client who can receive this information and document the client’s response in the record. Be sure that this is on a consent form signed by the client.
FAQ

Q: If the client is not conscious, to whom can we disclose the PHI?

You will have to decide this on a case-by-case basis. If you know the client's preferences, as in “you can tell my spouse, but not my sister,” then document the request and follow it. Otherwise, use your professional judgment. Always use the Minimum Necessary standard—disclose only information that is directly relevant to the person’s involvement with the client’s healthcare. Once a client has regained consciousness, he/she will determine when and how to share protected health information.
Multiple Choice

Question: You are working on a report that contains Protected Health Information and need to save the document to continue working on it. Where can you NOT save the document?

A. A departmental share drive
B. ServicePoint or other location designated by your program
C. A personal thumb or flash drive
D. On your home computer
E. The C drive of your laptop
F. C, D, and E
Social Media

- Your social media posts are a reflection on Volunteers of America of North Louisiana.
- “Employees should respect the privacy rights of their co-workers and the agency’s clients and must not disclose such information without obtaining permission from the Vice President of Communications and Development.”
- Employees must not post photographs and/or images of any co-workers, clients, volunteers, donors, or business partners on any social media site without having their expressed permission to do so…”

Personnel Policies
“Employees shall be expected to keep all information regarding the individuals served...confidential. “Keep confidential” is defined as safeguarding the content of written and verbal information including video, audio, and/or computer stored information from unauthorized disclosure without the specific informed consent of the individual, parent of a minor child, or legal guardian, and consistent with the advocate’s rights of access, as required in the Developmental Disabilities Act. All employees must comply with the confidentiality requirements of state and federal law concerning the identity and information related to Medicaid waiver clients.”
Technology and Social Media

• Employees may not...

• make public any proprietary or confidential information related to the agency, including clients, donors or volunteers (i.e. financial results, budget, strategic plan, intellectual property of the agency or personal client or employee information.), that is not already in the public domain.

• engage in any online conduct, which violates the agency’s conflicts of interest policies.

• post confidential information about third parties (i.e. community partners, funding sources, etc.)

• post or comment on program information, including but not limited to program closures, wish list, or updates on program status.
Technology and Social Media

Employees may not...

- recognize donors without prior consent from VP of Communications and Development.
- solicit for program donations of any kind.
- use Volunteers of America’s name, image, logo or abbreviation in any screen names or pages.
- create or manage any agency-related social media site (i.e. a Facebook page for your program).
Technology and Social Media

Employees should...

• respect the privacy rights of their coworkers and clients.

• use caution when “friending” or “following” a client or volunteer on social media, especially if they under the age of 18.

• refrain from posting or using written information related to the agency, agency logos or trademarks.
Technology and Social Media

• Employees should...
  • use a disclaimer such as, “the postings on this site are my own and do not represent the positions, strategies or opinions of Volunteers of America of North Louisiana.” when choosing to speak about the agency on any social media sites (i.e. a political opinion).
  • use discretion and your best judgment when making a post on any social media site.
  • report any employee to HR who believes a violation to our social media policy has occurred.
Crisis Communication

• “Employees should never participate in social media when the topic discussed may be considered a crisis. Even anonymous comments may be traced back to you or the agency’s IP address. Refer all social media activity topics to the Communications and Development department.”
FINAL EXAM!

Fill in the blank.

Knock Knock!
-Who's there?
HIPAA!
-HIPAA who?

someecards user card
More About HIPAA

U.S. Department of Health and Human Services

https://www.hhs.gov/hipaa/index.html

If you have questions or need additional information, visit the official website and take advantage of frequently updated resources there.
Thank you!
If you have completed this training, please notify Brad Campbell at charles.campbell@voanorthla.org in order for your participation to be recorded in your employee training file.
Other Sources


“Strategies to test your staff’s HIPAA knowledge…,” Nurse Manager Website, 5 December 2005.