HIPAA-HITECH and Computer Security Training

Health Insurance Portability and Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act of 2009

Introduction

Why We Are Here

Recently federal regulations that amend HIPAA/HITECH were finalized. Compliance with these new provisions is required by September 23, 2013. Therefore we are re-issuing our privacy training as many OPWDD employees handle this type of information in the course of our jobs.
Introduction

Why We Are Here

Protecting the privacy of the individuals we serve is a critical part of what we do at OPWDD. Privacy measures, when put into practice, contribute to a high standard of care and service we deliver to individuals with developmental disabilities.

Introduction

What You Will Learn

Upon successfully completing this training, the learner will understand:

1. The responsibility to keep certain information confidential
2. That taking appropriate measures can help safeguard information
3. That OPWDD takes privacy and confidentiality very seriously
4. Your responsibilities in the event of a breach of protected information
HIPAA Privacy Rule

The HIPAA Privacy Rule specifies "standards for privacy" of individually identifiable health information, called protected health information or PHI.

HIPAA Privacy Rule

Protected Health Information (PHI)

- PHI is individually identifiable health information that is stored and shared in ANY format, such as paper, electronic, oral, etc.

The information protected relates to:
- Past, present or future physical or mental health
- The provision of health care to a person, like a hospital record or physician notes
- Payment for health care provided to a person
HIPAA Privacy Rule

PHI For Our Purposes

- Clinical information under the Mental Hygiene Law is all information that relates to care and treatment
- Clinical information is considered PHI under HIPAA
- State or federal rules that provide greater confidentiality or access to individuals will prevail

HIPAA Privacy Rule

What Does the HIPAA Privacy Rule Do?

- Standardizes the rules for privacy across the country
- Balances the individual's privacy concerns with the public health concerns and responsibilities
- Gives people access to the information in their medical records and to how that information may be used
- Requires "covered entities" to keep records of with whom they have shared PHI, and make that available to the person, upon request
- Provides for monetary and criminal penalties for violations
HIPAA Privacy Rule

Applies to "Covered Entities"

Covered Entities are 3 types of organizations:

1. Health Plans
2. Health Care Clearinghouses
3. Health Care Providers

OPWDD is a covered entity, therefore HIPAA applies to OPWDD and its workforce members

Rights & Responsibilities

OPWDD Responsibilities related to HIPAA

1. Notify individuals of how their PHI may be used or shared
2. Notify individuals of their rights related to their records
3. Adopt and use its own internal privacy policy and procedures
4. Train all employees who are responsible for using, sharing or storing PHI and who handle complaints related to these functions
Rights & Responsibilities

OPWDD Responsibilities related to HIPAA

5. Assure agreements we have with contractors who handle PHI on OPWDD’s behalf outline the same privacy responsibilities as OPWDD.

6. Assist and assure that individuals are able to exercise their rights.

7. Establish appropriate administrative, technical and physical safeguards to protect PHI.

Rights & Responsibilities

5 A’s of Individual’s Rights under HIPAA

1. Access
2. Adequate Notice
3. Appeal
4. Amendment
5. Accounting
Rights & Responsibilities

5 A's of Individual's Rights under HIPAA

Right to Access their records:
People may read and get copies of their records for as long as the records are kept.

Right to Adequate Notice is the Notice of Privacy Practices:
Individuals must be notified, in plain language, of the following:

- How their PHI is likely to be used and shared
- Their rights under the HIPAA Privacy Rule
- The responsibilities of the covered entity related to PHI and the individual

The notice of Privacy Practices has been updated and redistributed to individuals who receive services from OPWDD.
Rights & Responsibilities

5 A's of Individual's Rights under HIPAA

Right to request Amendments be made to the records

The covered entity must consider, but may agree or disagree to make the amendment(s) requested.

Right to Appeal denial of access to records
Rights & Responsibilities

5 A's of Individual's Rights under HIPAA

The right to receive an Accounting of disclosures made.

Upon request, the covered entity must provide an accounting of certain types of disclosures of PHI, which must include specific information. This includes the disclosure of electronic health records. The six year “look back” time frame for which accounting of materials shared must be maintained.

Rights & Responsibilities

The Minimum Necessary Standard
Also known as "need to know"

The HIPAA Privacy Rule usually directs entities to limit the information shared to the minimum information necessary to carry out its functions.

There are two important exceptions to the Minimum Necessary Standard
Rights & Responsibilities

The **Minimum Necessary Standard** exceptions include:

1. The case where a provider needs the information to provide treatment to the individual
2. Times when disclosures are required by other laws

It is especially important to remember “need to know” when accessing electronic databases. Just because you can access information doesn’t mean you should. Do not search electronic databases for information you should not be accessing.
HITECH and Computer Security

The Health Information Technology for Economic and Clinical Health (HITECH)

The **purpose** of HITECH is to set national security standards for protecting certain health information that is **stored or transferred in electronic form**.

Internet/Email

Although there is no specific prohibition in HIPAA/HITECH for using the internet to transmit PHI, the internet is not secure.

Secure transmissions over the internet by using encryption, secure message systems or TLS.
HITECH and Computer Security

Unsecured and Secured Email

- If you need to email protected health information (PHI) or any type of confidential information over the Internet, there is a specific protocol that needs to be followed. Any email address that does not end with "@opwdd.ny.gov" is delivered over the Internet.

Here is a brief overview of the process for sending a message securely over the Internet:

- You need to add the word "secure:" (no need to type the quotes, just the characters in between them) in the subject line of your email.

- Please continue to the next page for examples.

Subject Line Examples:

Example 1:  
Subject: Secure: This message is secure!
This message will be sent securely because it contains the "Secure." text in the subject line.

Example 2:  
Subject: Secure: This message is not secure!
This message is NOT secure because there is a space between the word "Secure" and the colon ":", there cannot be a space present. The colon must directly follow the letter "e" for the message to be secure.

Example 3:  
Subject: This message is not secure!
This message is NOT secure when sent over the Internet (to non @opwdd.ny.gov email addresses). Email sent from one OPWDD email address to another is secure.
Key components of OPWDD's Computer Security Policy

- Systems and all data are the property of OPWDD and may be used for official business purposes only
- Use of computers, email and the internet is subject to provisions of OPWDD policies and State and Federal law
- Any use, authorized or not, constitutes express consent for OPWDD to monitor and record, or otherwise use, all activity
- Users of OPWDD computers and systems have no legitimate expectation of privacy

Key components of OPWDD's Computer Security Policy

- Access to information that identifies an individual receiving care or treatment in the OPWDD system is confidential under State Mental Hygiene Law and is Protected Health Information (PHI)
- Training is required annually for all OPWDD employees
- Computer Security Intranet Page
Computer Security Best Practices

- Log-off your computer when you are away from your desk
- Follow computer security policies for desktops, laptops, disks and other media; laptops are particularly vulnerable to theft and should be locked when not in use
- Use, but do not share, computer passwords
- Keep track of electronic devices which contain PHI. If you remove a paper or electronic file from your workstation, ensure it remains in your possession at all times
- When storing PHI, choose the most secure, accessible media: OPWDD system drives, hard drives and encrypted portable devices

Business Associates

Who IS a Business Associate?

A person or entity performing functions involving the use or disclosure of PHI on behalf of the covered entity.

These functions might be legal, actuarial, accounting, consulting, data collection, management, administration, accreditation or financial services
Business Associates

Who IS NOT a Business Associate?

- Health care providers other than those employed by the agency (for treatment purposes)
- Janitorial and cleaning providers
- US Postal Service workers and private carriers
- TRS Relay Services (telephones for the hearing impaired)

Business Associates

The Effect on Business Associates

- Business Associates are subject to direct fines for HIPAA violations
- Business Associates must comply with all administrative, technical and physical safeguards under the HIPAA Security Rule for e-PHI
- Business Associates must report breaches covered by the new notification rules and provide necessary information to the covered entity
What is Breach?

HIPAA-HITECH defines "breach" as unauthorized:

- Access to, or use or disclosure of, unsecured PHI
- Acts that compromise the security or privacy of the information

Breach

What is "Unsecured PHI"?

"Unsecured PHI" is PHI that is not:

- Encrypted
- Destroyed prior to disposal
- Rendered unreadable, unusable or indecipherable

This description includes both hard copy (paper) and electronic forms.
Breach

How Might a Breach Occur?

A breach may result from:

- Loss or theft of a device, such as a flash drive, laptop, smartphone, PDA, CD or DVD, etc., that contains PHI
- Files being stolen from your car
- Accidentally leaving files on the subway
- Loss or disclosure of paper documents to unauthorized individuals

Breach

A breach may also result from:

- Sending PHI to an incorrect address, e-mail address or fax number
- Posting PHI on an unsecured website, i.e. Facebook
- Unauthorized access of PHI from an application, database or another individual's private account
Breach

Notification for Breach of PHI

HIPAA HITECH Updates require covered entities to have procedures to:

- Report and identify unauthorized disclosures of unsecured PHI
- Assess the risk posed by such disclosures and determine whether an actual breach has occurred
- Notify individuals of a breach of their PHI in a timely manner, if a breach has actually occurred

Breach

What to do if Breach is Suspected

Immediate steps must be taken to ensure that proper and timely notification can, if necessary, be made to affected individuals, their representatives and to the appropriate oversight and regulatory agencies.
**Breach**

What to do if you are working and suspect that you have discovered a breach:

- **Immediately** notify your supervisor
- Your supervisor will notify the local information security officer (ISO) who will get in touch with you to learn the details of the suspected breach
- Do NOT discuss the possible breach with other employees or people outside of OPWDD. Please let the ISO complete his/her job!

**Breach Analysis**

The OPWDD HIPAA breach analysis template must be completed. Note that there is a presumption that a breach occurred unless after considering the following factors it determines there is a low probability the PHI was compromised

- Nature and extent of PHI
- Who is the unauthorized person who received the PHI
- Was the PHI actually viewed or acquired
- To what extent was the risk mitigated
Breach Analysis
Types of Safeguards

- **Administrative Safeguards** include putting in place policies and procedures for ways to keep PHI safe.

- **Technical Safeguards** are things like using a firewall, password-only access to files, secured networks for information transmission, etc.

- **Physical Safeguards** include things such as keeping paper data locked in cabinets, requiring ID’s to be shown before access to information is granted, etc.

Ask yourself how many times a day do you come in contact with an individual’s PHI?

If it were your information, how would you want it protected?
Risk Reduction

- Secure transmissions over the internet by using encryption, secure message systems or TLS
- Follow guidelines for email use
- Shred; don’t toss PHI housed on paper, CDs, and DVDs
- Use locked waste cans
- Do not store PHI on personally owned electronic devices and home computers
- Keep any files containing PHI, paper or electronic, with you at all times when you must take it from your workstation

Risk Reduction

- Follow facility security plans
- Use visitor sign-ins and escorts
- Shield computer work stations from public view and away from high traffic areas
- Provide training to all volunteers, interns, and outside contractors about their physical access responsibilities while at OPWDD facilities or those supported by OPWDD
Enforcement

- State Attorneys General may bring actions in Federal court for HIPAA violations
- Penalties can range from $100 to $1.5 million
- Business associates can be held directly liable
- Individual employees (workforce members) can face civil and criminal penalties
The HIPAA federal regulation applies to which type of information?

- A. Information about treatments received
- B. Information about diagnoses made for an individual
- C. Health information that is transmitted electronically
- D. Health information that is discussed orally
- E. Clinical Records
- F. Information that identifies individuals who receive services
- G. All of the above answers
- H. Only choices A and B above

Please match each of the 5 A's of Individual Rights to their definition by clicking on the word on the left and then clicking on it's definition on the right.

A. Appeal

B. Amendment

C. Accounting

D. Adequate Notice

E. Access

The right to know how one's PHI is used and shared, and what one's rights are under the HIPAA Privacy Rule

The right to inspect & obtain copies of one's own PHI

The right to receive a list of PHI disclosures and to whom they were made

The right to have a request that has been denied, reviewed

The right to challenge the accuracy of one's own PHI
Which are examples of appropriate safeguards?

- Using a user ID/password to access electronic records
- Locking file cabinets
- Shredding instead of tossing papers in trash bin
- Requiring visitors to sign in and be escorted

- A & C
- C & B
- All of the above

True or False? Under HIPAA HITECH covered entities, business associates, or workforce members who create a breach of PHI could be personally fined.

- True
- False
Which of the following would be considered unsecured PHI?

- A. Your encrypted work laptop that contains PHI
- B. Ten year old files containing PHI discarded in a hopper in the hallway during office clean out day
- C. Shredded PHI files sitting in an open trash can

Your OPWDD assigned laptop, which contains PHI, is missing from your work location. (You have already checked with your co-workers and nobody has seen the laptop.) What is your next step?

- Do nothing
- Continue looking for the laptop, but do not tell your supervisor about the situation
- Immediately inform your supervisor that your laptop is missing, and it contained PHI
A co-worker calls you at home and explains to you that she has forgotten her password to an OPWDD secure system. She asks you to share your user name and password with her, so she may log-in to complete a project before her boss gets mad because the project is not finished. (You are the only other person at the work location who has access to the system) What should you do?

- Share your user name and password
- Do not share your user name and password, but help your co-worker get in touch with the OPWDD IMS Help Desk
- Share your user name and password, but immediately change your password the next day

Which of the following should you do if you suspect a breach has occurred?

- A. Notify your supervisor before the end of your shift
- B. Send an email to your supervisor at your earliest convenience
- C. Inform your supervisor immediately
Congratulations!

You have completed the HIPAA-HITECH and Computer Security training.

In order to receive credit for this course, you must click on the button below, which will register your completion of this course in the Statewide Learning Management System.

Submit >