HIPAA Privacy and Security Training 2013

Produced by the Alabama Department of Public Health
Video Communications and Distance Learning Division

Faculty

Samarria Dunson
Assistant General Counsel
Alabama Department of Public Health

Topics of Discussion

- HIPAA overview
- Notice of Privacy Practices
- Disclosures of patient / client information
- Proper disposal of Protected Health Information (PHI)
- Patient / client rights

Topics of Discussion

- Reporting breaches of confidentiality
- Minimizing introduction of malicious computer software
- Proper use of passwords and / or system user names
- Responsibilities of e-PHI users

Topics of Discussion

- Reporting privacy and security breaches
- Sanctions for violations

Privacy Objectives

- Basic understanding of HIPAA privacy rules
- How to handle patient/client PHI both in paper and electronic form
- Reporting breaches of PHI
- Understanding the consequences of not following HIPAA regulations

What Is HIPAA and Why Is It Important?

- Health Information Portability and Accountability Act
- Background and purpose
- The Mega Rule

Civil Monetary Penalties

TABLE 2.–Categories of Violations and Respective Penalty Amounts Available

Violation Category – Section 1176(a)(1)	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
(A) Did Not Know	$100 - $50,000	$1,500,000
(B) Reasonable Cause	$1,000 - $50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000	$1,500,000

Criminal Penalties

- The American Recovery and Reinvestment Act of 2009 (ARRA) expanded HIPAA by providing that criminal penalties can be applied to employees and others who wrongfully disclose individually identifiable health information

Protected Health Information (PHI)

- Individually identifiable health information about an individuals past, present, or future medical or mental condition, transmitted or maintained in any form by a covered entity

Examples of Protected Health Information

- Name
- Address
- Date of Birth
- Date of Service
- Social Security Number
- Diagnosis
- Telephone Number
- E-mail Address

Examples of Protected Health Information

- Full face photographs and comparable images
- Medical Record Number
- Other information that would allow the patient / client to be identified

* Excludes employment and education records

ADPH Is a Hybrid Entity

- What does hybrid mean?
  - The Department has designated itself as a hybrid entity because it has divisions, bureaus, and clinics that provide direct patient care and others that do not

ADPH Is a Hybrid Entity

- Covered
- Support
- Non-covered

ADPH Is a Hybrid Entity

- The Department has decided ALL ADPH staff, whether they work for a covered, support, or non-covered division will be trained to comply with the HIPAA PRIVACY AND SECURITY RULES

HIPAA Exceptions

- Treatment
- Payment
- Operations

Quiz #1: Protected Health Information

Which of the following is are examples of protected health information?

a) Address

b) Date of Birth

c) Diagnosis

d) All of the above

Quiz #1: Answer

- d) All of the above
  - Protected Health Information is individually identifiable information that allows you to identify a patient
  - Common examples include:
    - Name, Social Security Number, Date of Birth, Date of Service, Address, and Telephone Number

Patient / Client Rights

- Obtain a copy of the Notice of Privacy Practices
- Request to view their own PHI
- Request to amend their PHI if they can prove that the information is inaccurate
- Authorize the Department to provide their information to someone else

Patient / Client Rights

- Limit the use and disclosure of their PHI
- Request an accounting of non-routine disclosures of PHI

Patient / Client Rights

- Make a complaint with the Department Privacy Officer of the Secretary of the Department of Health and Human Services if they feel that their rights have been violated

Notice of Privacy Practices (NOPP)

- The Department is required to provide a copy of the NOPP to all clients / patients
- The 2013 NOPP must be clearly posted for viewing in all Department clinics / bureaus / divisions that interact with patients / clients

Notice of Privacy Practices (NOPP)

- A copy of the 2013 NOPP can be found on the ADPH website at:
  - http://adph.org/publications/assets/Privacy.pdf

Uses and Disclosures of PHI: Patient / Client Access

- Viewing
  - Upon request, a patient / client has the right to view his / her PHI in a secure and non-obtrusive manner within the clinic
  - The request to view records can be in-person or in writing

Uses and Disclosures of PHI: Patient / Client Access

- Viewing must be noted in HIPAA Log and progress note or CHR1 Patient Log, whichever applicable

Uses and Disclosures of PHI: Patient / Client Access

- The law requires that the Department honor these requests within 30 days
  - 60 days if all of the records are not held at one location

Uses and Disclosures of PHI: Patient / Client Access

- EXCEPTION: Psychotherapy Notes (Social Work Notes)
  - A patient does not have the right to access psychotherapy notes
  - If this is an issue, contact the Privacy Officer for guidance

Uses and Disclosures of PHI: Patient / Client Access

- Copies of Records
  - Upon request, a patient / client has the right to a copy of their PHI
    - They can now request a copy in electronic form if the Department holds the information electronically (EHR)

Uses and Disclosures of PHI: Patient / Client Access

- All requests for copies of PHI should be completed within 30 days of the request
  - 60 days if the information is not contained in one location

Denying Access to PHI

- Reasons for denial include:
  - A licensed healthcare professional determines that access may endanger the life or physical safety of an individual
  - The information contains psychotherapy notes
  - Denials should be noted in the progress notes and the HIPAA Log

Denying Access to PHI

- The Department must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI to which access is denied
- In ALL circumstances, the Department's Privacy Officer MUST be notified prior to denying a request

Request by Patient to Amendment PHI

- Patients / clients may request that the Department amend their PHI if they believe their record contains an error or omission
- The Department is not obligated to make changes if information was not created by the Department or if information is accurate and complete

Request by Patient to Amendment PHI

- If a correction is appropriate, the Department must change all affected records to reflect the correction, notify the patient that the correction has been made and notify any providers that we are aware of for which we submitted incorrect data

Request by Patient to Amendment PHI

- All requests to amend PHI must be forwarded to the Department Privacy Officer immediately upon receipt
- Procedures for handling these requests are located in the 2013 HIPAA Privacy and Security Policy

Request by Patient to Limit PHI

- Patients / clients have the right to make reasonable requests to limit the release of PHI
- Requests to limit PHI should be made in the same manner as requests to alter or amend PHI

Request by Patient to Limit PHI

- All requests to limit PHI must be forwarded to the Department Privacy Officer immediately upon receipt
- Procedures for handling these requests are located in the 2013 HIPAA Privacy and Security Policy

Request by Patient for an Accounting of PHI

- Patients have a right to an accounting of their PHI
  - This means that they have a right to know to whom we have provided their information

Request by Patient for an Accounting of PHI

- An accounting of PHI is limited to non-routine disclosures
  - Non-routine disclosures include:
    - Subpoenas, releases to DHR and unauthorized releases
- Procedures for handling these requests are located in the 2013 HIPAA Privacy and Security Policy

Right to Confidential Communication

- Department clients / patients may sometimes request that we communicate with them in specific manners by using a specific phone number or mailing location
  - The Department must accommodate any reasonable request

Right to Confidential Communication

- To document this request, you must provide them with Form H of the 2013 HIPAA Privacy and Security policy

What Is the Minimum Necessary Rule?

- Department personnel who are directly involved in a patient's treatment and care (e.g., physicians, nurses, social workers and appropriate clerical workers) may have access to all of the patient's PHI

What Is the Minimum Necessary Rule?

- Department personnel who are not directly involved in a patient's treatment may not have unlimited access to a patient's PHI

What Is the Minimum Necessary Rule?

- It is a violation of the minimum necessary rule for a health care provider to access the PHI of patients with whom the provider has no treatment relationship, unless for research purposes as permitted by the Privacy Regulations and Department Policy

Exceptions to the Minimum Necessary Rule

The minimum necessary rule does not apply in the following instances:

1. Disclosures to, or requests by, a Health Care Provider for treatment
2. Uses or disclosures made to the patient or his / her legal representatives

Exceptions to the Minimum Necessary Rule

3. Uses or disclosures made pursuant to an authorization
4. Disclosures made to the Secretary of the U.S. Department of Health and Human Services for compliance and enforcement of the Privacy Regulations

Exceptions to the Minimum Necessary Rule

5. Uses and disclosures required by law
6. Uses and disclosures required by compliance with HIPAA standardized transactions

Uses and Disclosures of PHI: Staff Access

- Employees who are not directly involved in a patients care may NOT have access to a patients PHI
- Only ADPH employees, volunteers, and students involved in direct patient care are allowed to access a patient / client's PHI

Uses and Disclosures of PHI: Staff Access

- Even employees with a need to know the information must use the minimum necessary rule when viewing PHI

* Volunteers and students must have documented permission to view PHI

Quiz #2: Employee Access to PHI

When are Department employees allowed to view a patient's / client's medical record:

a) If an employee is personally familiar with the patient and needs their address to communicate with them about a church activity

Quiz #2: Employee Access to PHI

When are Department employees allowed to view a patient's / client's medical record:

b) If the patient / client is receiving medical treatment from the employee

Quiz #2: Employee Access to PHI

When are Department employees allowed to view a patient's / client's medical record:

c) All Department employees receive HIPAA training and therefore are allowed access to medical records kept by the Department

d) All of the above

Quiz #2: Answer

- b) If the patient / client is receiving medical treatment from the employee
  - Just because you are employed by the Department and receive training does not mean that you have the right to access patient / client information

Role of the Privacy Officer

- All covered entities must have a designated Privacy Officer
- The Privacy Officer is responsible for the following:
  - Assessing the Departments privacy issues
  - Implementing privacy policies and procedures

Role of the Privacy Officer

- Developing and implementing HIPAA training
- Resolving complaints and applying sanctions for HIPAA violations
- Ensuring that required documents are kept for six years

Role of the Security Officer

- All covered entities must have a designated Security Officer
- The Security Officer is responsible for the following:
  - Implementing security policies and procedures
  - Assisting with the development and implementing HIPAA training

Role of the Security Officer

- Overseeing the security of e-PHI
- Identifying and evaluating threats to the confidentiality and integrity of e-PHI
- Responding to actual or suspected breaches in the confidentiality or integrity of e-PHI

Security Objectives

- Secure electronic protected health information (e-PHI) at rest, while in ADPH custody
- Secure e-PHI in transit, both from and to ADPH
- Protect against reasonably anticipated threats to security and integrity of e-PHI and unauthorized access and use

Reviewing Policies and Procedures

- You should review the ADPH HIPAA Security policies and procedures for more detail about the safeguards we've implemented to protect e-PHI
- Contact your HIPAA Security Official with any questions regarding information security

Reviewing Policies and Procedures

- You will learn more about key steps you can take to safeguard e-PHI during the remainder of this presentation

Electronic Protected Health Information (e-PHI)

- e-PHI is information that is:
  - Electronically created
  - Electronically received
  - At rest or maintained in a storage device, such as a computer hard drive, disk, CD, or tape
  - In transit via the Internet, dial-up lines, etc.

Electronic Protected Health Information (e-PHI)

- e-PHI is not:
  - PHI that was not in electronic form before transmission, such as information shared by:
    - Person-to-person telephone calls
    - Copy machines
    - Paper-to-paper fax machines
    - Most voice mail

Electronic Protected Health Information (e-PHI)

- De-identified information is not e-PHI
- * The HIPAA Security Rule establishes standards for safeguarding e-PHI only

Major Security Risks

- Malicious computer software, such as viruses
- Unauthorized use of system user names and / or passwords
- Weak or ineffective passwords

Malicious Computer Software

- Malicious computer software can damage and disrupt Departmental computer systems by effecting the confidentiality, availability and integrity of e-PHI
- It gets into your computer from infected e-mail attachments, websites or diskettes, and CDs that contain malicious software

How to Protect Against Malicious Software

- Don't open e-mail attachments that look suspicious
- Report suspicious e-mails to the HIPAA Security Officer or IT staff
- Comply with instructions to update virus protection software

How to Protect Against Malicious Software

- Never copy or download software without permission from your supervisor
- Never disable or tamper with virus protection software
- Make sure that any computer or laptop that you use has up to date virus protection

Quiz #3: Reporting Security Incidents

- Whenever a Department employee suspects that there is a security incident relating to malicious software, they should immediately report it to which of the following:

Quiz #3: Reporting Security Incidents

a) The website that was the source of the download

b) The HIPAA Security Officer

c) The HIPAA Computer Compliance Officer

d) No one and delete the link to the information immediately

Quiz #3: Answer

- b) The HIPAA Security Officer
  - This suspicion should be reported to the HIPAA Security Officer immediately so that she can work to minimize the harm done by a malicious software attack

Quiz #4: Alerts and Updates

- True or False
  - If you receive an alert or update from an ADPH IT staff member, you should immediately open it, read it, and follow all of the instructions

Quiz #4: Answer

- True
  - The alerts and updates greatly assist Departmental IT staff with reducing issues relating to malicious software

Mobile Devices

- Cell Phones
- Laptops
- Flash Drives
- HHS Recommendations

Topics for Discussion

- Fax Procedures
- E-mailing / Texting
- Social Media

HIPAA Privacy and Security Officers

Privacy Officer:

Samarria Dunson

P.O. Box 303017

Montgomery, AL 36130 – 3017

334 – 206 – 5209

Samarria.Dunson@adph.state.al.us

HIPAA Privacy and Security Officers

Security Officer:

Cheryl Perez

P.O. Box 03017

Montgomery, AL 36130 – 3017

334 – 206 – 5064

Cheryl.Perez@adph.state.al.us