HIPAA and Privacy Policy Training

July 2015

Overview of Training

This training addresses the requirements for maintaining the privacy of confidential information received from HFS and DHS (the Agencies).

During this training you will learn:

* The definition of confidential information;
* The basic requirements of the laws that restrict how confidential information can be accessed, used, and shared;
* Practical ways to protect the privacy and security of confidential information; and
* The consequences if you improperly access, use, or share confidential information. Possible sanctions include:
  * Losing your job;
  * Monetary fines; and
  * Imprisonment.

Confidential Information

Confidential Information is defined by several laws, including:

* HIPAA (45 CFR Parts 160, 162, and 164)
* Federal Medicaid Confidentiality (42 CFR 431.300-307)
* Personal Information Protection Act (815 ILCS 530)
* Identity Protection Act (5 ILCS 179)
* Child Support Confidentiality (45 CFR 303.21, among others)
* IRS Code (IRC 6103)
* Illinois Public Aid Code (305 ILCS 5/11-9)

Confidential Information - The General Rules

1. All client information collected or received by the Agencies is CONFIDENTIAL.

2. Every employee, agent, and contractor of the Agencies, and every other person or entity who receives the Agencies' client information, must protect the privacy and security of client information.

The Agencies' clients include applicants and beneficiaries.

Confidential Information - The General Rules

Examples of confidential information to be protected:

* Name
* Address
* Phone number
* Date of Birth
* Recipient Identification Number
* Social Security Number
* Driver's License Number
* Financial Information, including account numbers

HIPAA

The Health Insurance Portability and Accountability Act

HIPAA – An Overview

The Agencies are "covered entities" under HIPAA. This means that the Agencies, their employees, their agents, their contractors, and anyone else who receives the Agencies' client information must comply with HIPAA's rules.

HIPAA provides the most basic legal protection for health information. Other laws can add more protection. The Agencies, and anyone who receives the Agencies' data, must comply with all of these laws.

HIPAA – An Overview

HIPAA requires the Agencies to safeguard their clients'

Protected **H**ealth **I**nformation (PHI).

HIPAA – PHI

PHI is information that:

* identifies an individual (or can be used to identify an individual); and
* relates to the health, payment for, or provision of healthcare to an individual.

PHI can be in any form:

* Electronic, including email
* Paper
* Spoken

HIPAA – PHI

PHI can even include basic, non-medical information. In fact, any of the following are considered identifiers, and are therefore PHI under HIPAA:

* Names
* Any geographic area smaller than a state
* Telephone numbers
* Fax numbers
* Email addresses
* Age (if over 89)
* Social Security Numbers
* RINs
* Dates (except year)
* Names of relatives
* Account numbers
* Any other unique number that can be linked to an individual

HIPAA
Use and Disclosure of PHI

HIPAA governs:

* how the Agencies can **access** and **use** PHI internally; and
* when the Agencies can **share (disclose)** PHI with external persons or entities.

The following slides provide examples of the most common acceptable uses and disclosures of PHI.

HIPAA

Authorized Uses and Disclosures of PHI

Example 1: Consent

The Agencies can use and disclose PHI with the written consent of the client.

However, you must stay within the boundaries of the consent.**

**Common issues to look for include:

- The expiration date of the consent; and
- The purpose of the consent.

HIPAA

Authorized Uses and Disclosures of PHI

Example 2: Treatment, Payment, and Healthcare Operations of the Agencies (TPO)

The Agencies can use and disclose PHI for their TPO activities, without obtaining a client's written consent.

TPO includes:

* Accessing PHI to perform your job
* Determinations of eligibility
* Billing
* Care coordination activities
* Quality assessment and improvement activities
* Review of the competence and qualifications of health care professionals
* Review of health care services and utilization
* Fraud and abuse detection.

HIPAA
Authorized Uses and Disclosures of PHI

Example 3: TPO of Another Covered Entity

The Agencies can use and disclose PHI for:

* The treatment activities of another health care provider;
* The payment activities of another covered entity; and
* The healthcare operations of another covered entity, provided certain factors are met.

Written consent from the client is not necessary for these disclosures.

HIPAA

Authorized Uses and Disclosures of PHI

Other Permissible Situations

HIPAA also allows disclosure of PHI in the following situations:

* Health oversight activities
* Judicial and administrative proceedings
* Law enforcement purposes
* National security
* Research
* Requests from other covered entities administering government programs or providing public benefits

Each situation listed above must meet specific criteria before PHI can be disclosed.

DO NOT DISCLOSE PHI under one of the situations listed above without written permission from the Agencies.

HIPAA

Authorized Uses and Disclosures of PHI

Your entity, as a recipient of the Agencies' client information, is permitted to access and use the information only for the purpose for which it was shared and in compliance with HIPAA.

HIPAA

Authorized Uses and Disclosures of PHI

Never disclose the Agencies' client information to a person outside of your organization without talking to your supervisor first. Your supervisor may need to contact the Agencies for permission to disclose the information.

This includes requests for PHI from law enforcement or public officials!

HIPAA

Authorized Uses and Disclosures of PHI

Minimum Necessary

Use only the minimum amount of PHI necessary to perform your job.

The “minimum necessary” standard does not apply to disclosures made to the client or his/her representative.

HIPAA – Breach Defined

A breach under HIPAA occurs when there is an:

Unauthorized access, use, or disclosure of PHI that compromises the security or privacy of the PHI.

HIPAA – Breach Penalties

You can be held personally accountable for a violation of HIPAA.

This includes:

Disciplinary Action at Work

Monetary Fines

Imprisonment

Your actions could also subject your employer and the Agencies to monetary penalties and negative media coverage.

HIPAA – Breach Penalties

Penalties for HIPAA violations include:

* Civil penalties:
  * Monetary fines range from $100 to $50,000 per violation.
  * The amount of the fine depends on (1) whether the violation is corrected within 30 days; and (2) whether the violation is due to willful neglect or reasonable cause.

* Criminal penalties:
  * A knowing violation = up to $50,000 fine and 1 year in prison.
  * A false pretenses violation = up to $100,000 fine and 5 years in prison.
  * An intent to use for personal gain or malicious harm = up to $250,000 and 10 years in prison.

Examples of Real-Life HIPAA Penalties

* A UCLA Health System employee was sentenced to 4 months in federal prison and fined $2,000 for accessing and reading the confidential medical records of his supervisors and high-profile celebrities.
* A South Carolina state employee was sentenced to 3 years probation and community service for sending personal information about Medicaid recipients to his personal email account.
* A Texas hospital employee was sentenced to 18 months in federal prison and ordered to pay $12,152 for wrongful disclosure of PHI and intent to use PHI for personal gain.
* Walgreens was ordered to pay $1.44 million to a customer whose PHI was impermissibly accessed and disclosed by a pharmacy employee who suspected her husband's mistress had given him a sexually transmitted disease.
* A Massachusetts health care provider agreed to pay $1.5 million to settle HIPAA violations that included the theft of an unencrypted personal laptop that contained electronic PHI.
* A small, single-location pharmacy agreed to pay a $125,000 fine for disposing of documents containing PHI in its dumpsters, without shredding or rendering the documents unreadable.

HIPAA – Breach Examples

Unauthorized Access

If you access PHI without a job-related reason for doing so, you have violated HIPAA.

* For example, you violate HIPAA if you use the Agencies' systems to look up the phone number or address of someone you suspect is having an affair with your spouse.

* You also violate HIPAA if you are "just curious" and use the Agencies' systems to access information about your friend.

If you are not performing a job function or do not have written authorization, then you may not access a client's information.

HIPAA – Breach Examples

Unauthorized Use

If you use PHI in any manner that is not related to your job duties, you have violated HIPAA.

* For example, as part of your job you must access client information from the Agencies' computer system. While performing your job you see that a person you know and dislike suffers from an embarrassing medical condition. You use this information for personal gain by blackmailing the individual, or you reveal this information to embarrass the individual. Both actions are breaches under HIPAA.

* You use a client's name, birth date, and Social Security number to fraudulently obtain credit cards. This type of breach is punishable under HIPAA by up to 10 years in prison and a $250,000 fine.

HIPAA – Breach Examples

Improper Disposal

If you dispose of PHI in a manner that does not render it unreadable or unusable, you have violated HIPAA.

* For example, you print documents that contain PHI as part of your job duties. Instead of shredding the documents after you are done using them, you place them in a bin on the floor to be shredded later and leave for the night. The night cleaning crew mistakes your shred bin as garbage and empties it into the regular trash.

HIPAA – Breach Examples

Lost or Stolen Information

If you lose documents or hardware that contain PHI that is not encrypted or secured, or the documents or hardware are stolen, a breach of HIPAA has occurred.

* For example, you mail documents containing PHI that never make it to the intended recipient. This is a HIPAA breach.

* You leave your laptop in your car, and the car is stolen. Although the laptop is password protected and the hard drive is encrypted, you wrote the password down and kept it next to the laptop. This is a HIPAA breach.

HIPAA – Breach Examples

Unauthorized Disclosure

If you disclose PHI in a manner that is not allowed by HIPAA, you have violated HIPAA.

* For example, while performing your job duties you learn that your neighbor is receiving Medicaid and is taking medication for depression. You tell this information to your spouse.

* You disclose PHI in response to a subpoena. The subpoena was not accompanied by a HIPAA compliant Court Order or any other documentation required by HIPAA.

** Always refer subpoenas and Court Orders requesting client information to the Agencies.

Reporting an Incident

You must report any suspected privacy breaches to the HIPAA/Privacy Officer immediately. Examples of things to report:

* Unauthorized access, use, or disclosure;
* Loss, theft, or improper disposal of papers or devices that contain PHI; and
* Unsecured emails containing PHI.

The Privacy Officer will investigate whether a breach has occurred and determine what notifications are necessary.

In some instances, the Privacy Officer must notify State officials, Federal officials, the affected individuals, and the media. The letters of explanation will describe the circumstances of the breach and may include the names of responsible parties.

Every breach costs the Agencies a significant amount of money and resources and has the potential to harm the reputation of the Agencies.

HIPAA – Individual Rights

HIPAA also gives individuals certain rights, including:

* The right to access their health information;
* The right to amend their health information;
* The right to alternative means of communication (different mailing address, language, etc.);
* The right to restrict uses and disclosures of their health information;
* The right to file a complaint; and
* The right to receive an accounting of disclosures.

Immediately refer these requests to the HIPAA/Privacy Officer. These requests are time sensitive.

HIPAA – Right to an Accounting

If a client requests an accounting, HFS must provide a list of all disclosures it made in the prior 6 years except for the following types of disclosures:

* Disclosures made for TPO purposes;
* Disclosures made to the individual (or the individual's representative);
* Disclosures pursuant to authorization;
* Disclosures as part of a limited data set;
* Disclosures for national security or intelligence purposes;
* Disclosures to correctional institutions or law enforcement officials for certain purposes regarding inmates; and
* Disclosures incidental to otherwise permitted or required uses or disclosures.

All other disclosures must be accounted for. Contact the Privacy Officer before you make any other type of disclosure.

Beyond HIPAA – Other Confidentiality Laws

The Agencies are subject to several other confidentiality laws, including:

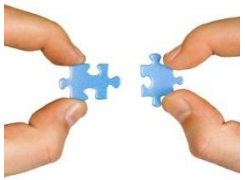
* Medicaid Confidentiality Rules and Regulations
* Illinois Identity Protection Act
* Illinois Personal Information Protection Act
* Heightened Confidentiality Laws (mental health, substance abuse)

Medicaid Confidentiality Rules and Regulations

Federal and State Medicaid confidentiality laws prohibit the Agencies from disclosing any information about a client unless the disclosure is directly connected with the administration of public assistance.

Purposes directly connected with the administration of the public assistance include:

* Establishing eligibility;
* Determining the amount of assistance;
* Providing services; and
* Conducting or assisting in an investigation or proceeding related to the administration of public assistance.



Illinois Identity Protection Act

The Identity Protection Act protects Social Security Numbers (SSNs) by prohibiting State agencies from doing certain things, including:

* Printing SSNs on cards required to access services or products;
* Requiring an individual to transmit SSNs over the internet (unless the connection is secure and encrypted); and
* Limiting how State Agencies use and disclose SSNs.

Bottom Line: Be extremely careful when using or sharing SSNs. Before sharing SSNs with anyone, ask yourself whether it is necessary to share that piece of information. If it is, ask the Privacy Officer if it is permissible.

Personal Information Protection Act

The Personal Information Protection Act requires the Agencies to notify individuals and the General Assembly when there has been a breach of a client's name in combination with one of the following:

* Social Security Number;
* Driver's license or State identification card number; or
* Account, credit card, or debit card number.

The Act also imposes penalties for improper disposal of written or electronic material that contains personal information. Penalties range from $100 to $50,000 and can be imposed on the individual, not just the Agencies.

Child Support Rules and Regulations

Federal laws prohibit HFS and its employees from disclosing information related to the child support program, except in extremely limited circumstances.

* Confidential Information in the child support context means any information related to the individual, including name, address, SSN, employment information, and financial information.
* You should assume any information obtained by or from the child support program is confidential.

The IRS also imposes harsh penalties for the unauthorized inspection or disclosure of Federal Tax Information (FTI).

* FTI is any information derived from a tax return received from the IRS. FTI is strictly confidential and may be disclosed only in very limited circumstances.
* FTI does not include information provided directly by the taxpayer.
* An unauthorized disclosure of FTI occurs when FTI is provided to an individual who does not have the statutory right to have access to it. The unauthorized disclosure of FTI is a felony punishable by fines, imprisonment, or both.
* An unauthorized access of FTI occurs when an entity or individual has access to FTI without authority. The unauthorized access of FTI is a misdemeanor punishable by fines, imprisonment, or both.
* Unauthorized access or disclosure requires immediate notification to the HFS Privacy Officer, who must in turn immediately notify the IRS.

IRS

Illinois Public Aid Code

The Illinois Public Aid Code prohibits Illinois state agencies, county, and local governmental units from disclosing any information related to individuals who applied for or receive public assistance.

* You should assume any information obtained by or from any public aid program, including Supplemental Nutrition Assistance Program (SNAP) or the Temporary Assistance for Needy Families (TANF) is confidential.

* Confidential Information includes any records, files, papers, and communications concerning an applicant, regardless of whether the applicant was approved or denied.

The Public Aid Code restricts the disclosure of such information ONLY for purposes directly connected with the administration of public aid.

Federal laws also impose harsh penalties for unauthorized disclosure of any information relating to people who applied or receive SNAP or TANF benefits.

Other Confidentiality Laws

HIPAA provides the least restrictive confidentiality laws related to health information privacy.

Some areas of healthcare are deemed more sensitive than others and therefore have more restrictive privacy laws. For example:

* Substance Abuse Information: Federal law severely limits the ability to share any information regarding substance abuse treatment without the patient's consent.
* Mental Health: State law limits the ability to share mental health treatment information without the patient's consent.

When dealing with these areas, be sure to familiarize yourself with the confidentiality restrictions. If you have questions, contact the Privacy Officer.

How to Avoid a Breach

Simple steps you should take to secure confidential information:

Workstation

* Prevent visitors from viewing documents or computer screens containing confidential information.
* When leaving your workstation for a break, lock your computer and conceal documents containing confidential information.
* When leaving your workstation for the day, place documents containing confidential information in locked file cabinets or behind a locked door, if available.

How to Avoid a Breach

Paper Documents

* Avoid printing documents containing confidential information when possible.
* Do not place documents containing confidential information in the trash or on the floor of your workstation.
* Shred documents containing confidential information immediately when you have finished using them.
* Before mailing any documents, double check to make sure the envelope is properly addressed and only the intended documents are included in the envelope.

How to Avoid a Breach

Faxing

* Confirm the fax number before sending.
* Confirm that the recipient's fax machine is in a secure location.

How to Avoid a Breach

Email

* Avoid sending email containing confidential information. This includes an email that contains just the client's name and no other identifying information.

* If you must send an email containing confidential information, secure the email and password protect attachments.

* When responding to emails, always check the contents of the email string and attachments for confidential information before sending. If possible, send a new email as your response.

How to Avoid a Breach

Personal Devices

* Never store confidential information on a personal mobile device (laptop, phone, memory stick, etc.).

* Never email confidential information to your personal email account.

Things to Remember

* Confidential Information exists in printed, electronic, and spoken forms.
* Confidential Information includes client names, addresses, date of birth, SSNs, credit card and driver's license numbers, federal tax information, and PHI.
* You must have the client's written authorization or a job related reason to access, use, or disclose the client's information.
* Access, use, and disclose only the minimum amount of confidential information necessary to do your job.
* Always double check the contents and recipients of an email. Secure any emails containing confidential information.
* Always double check the contents of mailings that contain confidential information to ensure only the intended materials are included and the envelope is correctly addressed.

HIPAA/Privacy Officer

If you have questions regarding confidential information:

* Discuss with your supervisor
* Contact the Agencies' HIPAA/Privacy Officers

Elizabeth Festa
Healthcare and Family Services
Office of the General Counsel
(312) 793-4805
HFS.Privacy.Officer@illinois.gov

Tola Sobitan
Human Services
Office of the General Counsel
(312) 814-8756
DHS.HIPAA@illinois.gov

Now that you have finished the show….

Follow these instructions to confirm your completion of the HIPAA training requirement:

- ☑ **Click on the link below to access the confirmation form**
- ☑ **Follow the form instructions for completion**
- ☑ **Print and sign the form**
- ☑ **Submit it to your supervisor**

HIPAA Privacy Policy Training Attestation Form (DOC)