LUTHERAN CHILD AND FAMILY SERVICES OF ILLINOIS

HIPAA TRAINING PART 1

MARCH 2003

TABLE OF CONTENTS

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act (1996). The Federal Government describes HIPAA as "administrative simplification". It's an opportunity to standardize the electronic data interchange in the healthcare industry. This should lead to reduced operational costs and improve the quality in which information is exchanged.

There are three standards of HIPAA:

-Transactions and Code Sets
-Privacy
-Security

HIPAA protects the integrity, privacy, and security of healthcare data by enforcing privacy regulations in healthcare and other industries.

Part of the HIPAA requirement is to provide training on the regulations to all current and future employees. **The focus of this training document is the protection of the confidentiality of health information.**

HIPAA enforces privacy regulations within healthcare and other industries that:

- Protect an individual's identifiable medical history and condition.
- Gives clients the right to know who has or will see their records (for purposes other than treatment, payment and health care operations).
- Provides the same level of protection for all confidential information.
- Creates a "federal floor" of privacy protection but would not supercede state laws providing greater protection.

Why do you need to know about HIPAA?

During the course of your job here at LCFS, whether you intend to or not, you come in contact with information about the health status of clients. That information is private information, and we have treated it that way for many years. HIPAA has created additional privacy regulations to ensure the safeguarding of that type of information, which we have incorporated into our way of doing things. In this packet we will discuss those ways, and how they impact you. Additional aspects that are new with HIPAA, something everyone in healthcare should know about, are the potential penalties that an individual can incur for violations to HIPAA, also known as breaches in confidentiality. The potential penalties for such a violation are as follows:

Criminal Penalties: It is a Federal crime for anyone to knowingly and wrongfully disclose or receive individually identifiable health information in violation of HIPAA.

- Fines: $50,000 to $250,000
- Imprisonment 1 to 10 years.
- Both civil and criminal penalties may be imposed.

Civil Monetary Penalties: For each failure to comply with each HIPAA provision - $100 per violation, capped at $25,000 for violations of the same provision.

What Exactly do we Need to Protect?

Part of the reason that HIPAA was enacted was to help safeguard the Protected Health Information (PHI) of clients and other persons that is generated by a healthcare provider or other institutions.

What is PHI?

Through the course of our daily business, Lutheran Child & Family Services of Illinois (LCFS), as well as all other healthcare providers and many other businesses generate or receive information about the condition, past, present, and future of the clients that we and they treat. Once this information becomes linked with the identity of the person being treated, it becomes Protected Health Information (PHI). PHI is information that ...

- ✓ identifies an individual by name, number, characteristic or code.
- ✓ relates to the services provided to a client by LCFS (past, present or future) is maintained or disclosed electronically, on paper or orally.

"Individually identifiable" means that someone seeing or hearing this information can identify the person it's about. Certain information is unique to an individual and by itself can identify that person. If information is linked with the following unique items, it is considered PHI:

- ✓ Name
- ✓ Social Security Number
- ✓ Drivers License Number
- ✓ Telephone or Fax Number
- ✓ Address
- ✓ Email address or URL
- ✓ Client ID Number
- ✓ Account Number or Health Plan Number
- ✓ Biometric Identifiers (Finger Print/Voice Print)
- ✓ Photograph or Likeness
- ✓ Date of Birth
- ✓ Name of Relatives
- ✓ Employer
- ✓ Insurance Information
- ✓ Codes
- ✓ Certificate Number

PHI Examples

Written PHI

- ✓ Client's record
- ✓ Sign in sheet with client's name and reason for visit
- ✓ A code that documents a specific service or test LCFS provides
- ✓ Client's insurance card.

Oral PHI

- ✓ A conversation about a client's condition with a colleague in a place where others can overhear
- ✓ An appointment reminder message on an answering machine
- ✓ A telephone call to verify health insurance coverage
- ✓ A client report dictated onto a tape.
- ✓ Calling out a client's full name and reason for the visit in a waiting room.

Paper PHI

- ✓ Fax sheets
- ✓ Face sheets or client information from hospitals, physicians, DCFS, court, schools, etc..
- ✓ Test results

Computer/Other Media PHI

- ✓ Data appearing on computer monitors and screens
- ✓ E-mail with PHI included in it.
- ✓ Palm Pilots with stored PHI in it.
- ✓ Photos
- ✓ CD's and Tapes

What are the Permitted Uses and Disclosures of PHI?

There are times when employees are permitted to use or disclose PHI, such as in the course of TPO.

What is TPO ?

TPO is the acronym for Treatment, Payment, and Healthcare Operations.

Treatment is defined as the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination and management of healthcare and related services by one or more healthcare provider, and includes the coordination and management of healthcare by a healthcare provider with a third party. Treatment includes:

Consultation among providers
Assistance by telephone
Referrals from one provider to another

Payment is defined as activities by a healthcare provider or a health plan to obtain or provide reimbursement for the provision of healthcare. Examples are:

Determination of eligibility or coverage
Billing
Claims Management
Collection Activities
Utilization Review Activities

Client Service Operations is defined as activities which are directly related to treatment/ service provision or payment. These are activities which are necessary for treatment or payment to occur. Examples are:

Quality Assessment and Improvement Activities
Client Service Coordination/ Case Management
Client Service Planning
Training, Accreditation, Certification, Licensing, Credentialing or other related activities
Service Review and Auditing Functions

Uses of PHI

Use describes how PHI is used and shared on a daily basis **within the organization.**

Permitted uses of PHI are:

Sharing, employing, applying, utilizing, examining or analyzing of **information inside the agency that maintains PHI.**

Disclosure of PHI for other than TPO

Disclosure describes how PHI is released, transferred or accessed **outside of the organization for other than TPO.**

Permitted disclosures are:

Release, transfer or provision of access to PHI outside of the organization for **other than treatment, payment, or healthcare operations (TPO), however, authorization is required.**

Authorization

An authorization is a form that outlines a request to release various elements of PHI to a specific party outlining the purpose of the disclosure. It is usually completed by the client and follows a prescribed process.

Authorization is **required** when disclosing information for **other than Treatment, Payment and Healthcare Operations (TPO)** for:

Disclosure of Protected Health Information (PHI)
Marketing
Fundraising
Must be in writing

The client has the right to revoke authorization

Specific situations exist when uses and disclosures can be made without an authorization. Examples are:

For public health activities such as the purpose of controlling disease, injury or disability, and
Abuse, neglect, or domestic violence to a governmental authority, and
As required by law

Except for these permitted disclosures, PHI is not to be disclosed without an authorization. Some examples of unauthorized disclosures would be:

An incoming phone call inquiring about a client, and
Talking to your spouse or neighbor about a client

Who is Authorized to Access Protected Health Information?

- Health Care Providers involved in the treatment of the client, (counselor, nurse, physician etc.)
- The client, with a signed authorization
- Anyone authorized in writing by the client
- All staff, if necessary to carry out their job duties and responsibilities
- Business Associates, if necessary to carry out their job duties and responsibilities

Minimum Necessary Standard

HIPAA privacy regulations clearly state that use and disclosure of PHI should follow the minimum necessary standard to fulfill a request or to perform the job.

Consider the following questions:
-How much information do you need to perform your job?
-How much information does the requester need to perform their job?

How Can We Protect PHI?

-Be aware of your surroundings when using the phone or talking to co-workers
-Never have client charts out in the open
-Close office doors when unoccupied
-Interoffice Mail- All confidential information must be in a sealed envelope
-Keep file cabinets containing PHI closed and locked when not in use.
-**What you see and hear in the workplace is confidential- so keep it to yourself**

Ways to Protect Electronic Data- Faxing

If you are authorized to fax PHI:
-Determine what PHI should be faxed
emergent client situations
pre-authorization for services
to internal departments

Always use an approved cover sheet
Make sure to validate the fax number prior to sending the fax
Whenever possible store the fax number in your fax machine's memory

Security Reminders

Sharing passwords is prohibited
Workstations should be positioned so that displays can not be seen by unauthorized individuals
Computer users need to exit to a menu or generic display when done with their transactions
Computer users must log off when leaving the work area

Notice of Privacy for Clients

HIPAA requires healthcare providers to provide notice to clients/clients on how their information usually will be used.

Prior to delivery of service, all clients/clients must receive LCFS' **Notice of Privacy Practices.**

LCFS' **Notice of Privacy Practices** is attached to this document.

Client Access to PHI

- ✓ PHI can only be accessed by the client receiving care. In some circumstances it may be appropriate for a parent, guardian, legal custodian of a minor, spouse or legal representative of a deceased person, or healthcare agent designated by an incapacitated person to be granted access to PHI.
- ✓ The individual has the right to view or make a copy of his/her PHI, but the original source PHI shall not be removed from the system.
- ✓ In some circumstances parents, legal guardians, or others described above can be restricted from PHI. **See full policy for details.**

What is the Process for Requesting PHI?

- ✓ Requests to access PHI, must be in writing as defined in LCFS' **Notice of Privacy Practices.**
- ✓ LCFS has 30 days to respond to the request. If the request is denied, reason for the denial will be provided. If the request is delayed, reason for the delay will be provided.
- ✓ LCFS can deny access without the appeal of the requestor in the event that the PHI was not created by LCFS, or the event that access to the PHI could reasonably endanger the life or safety of another person.

Amendment of PHI

One important aspect of HIPAA is that clients not only have a right to access their PHI, but they also have the right to review and request an amendment of their PHI should the need arise. **See full policy for details.**

Privacy Officer

The Director of Quality, Susan Stephens, will also assume the duties of the Privacy Officer. The Privacy Officer

- Monitors compliance with privacy policies and procedures
- Monitors privacy practices in accordance with state and federal laws
- Follows up on all reports of potential privacy violations

Who Should I Report Breaches/Violations to?

It is important to remember that complying with HIPAA is everyone's obligation. What should you do if you observe a violation of these regulations or have been told about a violation? If there was a complaint from a client or family member, they should be directed to the Privacy Officer. If you have any questions or concerns about HIPAA policies or practices, contact your direct supervisor or the Privacy Officer.

Clients and members of the public may also report violations to the supervisor and the Privacy Officer.

Violations can also be reported to the Department of Health and Human Services (DHHS) Office of Civil Rights (who may interview staff and review policies and procedures). Many times the complaint may be based on a misconception so it is encouraged to have the complaint addressed to the Privacy Officer first.

Based on the circumstances and investigation there could be internal penalties, sanctions or for more serious breaches, civil and criminal penalties.

Summary

HIPAA requires detailed policies and procedures in place that dictate how client information

- Is to be used
- When it can be disclosed
- How it should be disposed of

All staff will need to be familiar with these policies, particularly those pertinent to their department or job responsibilities.