Dallas Children's Advocacy Center

Dallas Children's Advocacy Center

PROVIDING JUSTICE • RESTORING HOPE

HIPAA Overview

- As an employee of DCAC, you must understand how the Health Insurance Portability and Accountability Act (HIPAA) impacts clients, employees and the agency. Federal standards authorize a fine and/or imprisonment of organizations and individuals for each offense of wrongful disclosure of protected health information (PHI).
- If you fail to protect privacy, the HIPAA regulations allow you and/or DCAC to be fined $100 per violation, up to $50,000 per person per year for each requirement or prohibition violated. Repeat and uncorrected violations can extend up to $1.5 million in fines.
- Criminal penalties may also be imposed. You could pay up to $250,000 in criminal fines and serve up to ten years in prison.

HIPAA Overview

OBJECTIVES

- After completing this course, you should be able to:
- Describe the purpose and the importance of HIPAA rules.
- Define protected health information (PHI), privacy and security with regard to client information.
- Define appropriate uses for PHI.
- Describe the HIPAA privacy rule and list elements required of the privacy
- notice.
- Describe the “minimum necessary” requirement and when to use it to protect PHI.
- Identify potential threats to the security and privacy of client information.
- Identify and describe ways DCAC safeguards PHI.
- Understand the consequences of an individual’s and organization’s violation of HIPAA rules and regulations.

Purpose of Ethical Code of Conduct

HIPAA IS A REGULATION THAT IMPACTS THE ENTIRE ORGANIZATION, INCLUDING:

- Client communication
- Business processes
- Policies and procedures
- Technology
- Contracts, grants or funding sources that involve the use and disclosure of PHI

HIPAA AFFECTS DAILY TRANSACTIONS SUCH AS:

- Client sign in procedures
- ETO data entry
- VPN use off site
- Coordination of care with partners
- Internal and external communications
- Referral for resources
- Client care and safety
- Faxing client information

HIPAA Overview

To understand your role with regard to HIPAA, you must first know what comprises protected health information (PHI) and the difference between privacy and security.

- Privacy: An individual's interest to protect his or her personal information from inappropriate access by others. State and federal laws, including the Privacy Rule adopted as part of HIPAA, outline the use and disclosure of client information.
- Protected Health Information: When information: 1.) is related to the health of or healthcare received by a person; and 2.) identifies a person or could be used to identify a person, it is considered protected health information (PHI)
- Security: Assures that privacy is maintained by preventing the accidental or intentional use of client health information by unauthorized users. The Security Rule as part of HIPAA sets standards for the security of electronic protected health information.

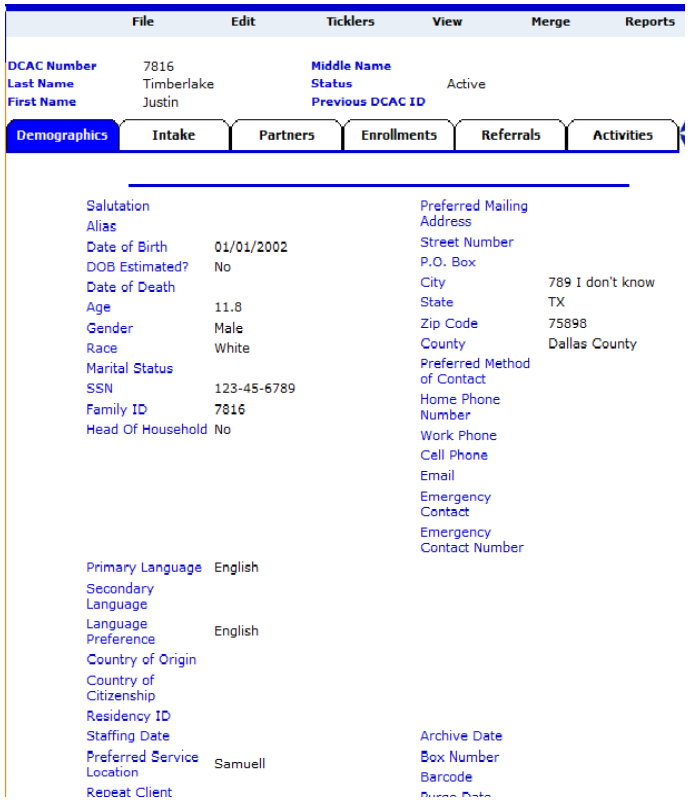
HIPAA Overview

If you can link information to a client's identity, then the information must be protected.

Can you identify all instances of PHI in this electronic record?

Remember: Patient information can be found in many places and communicated in many ways, including:

- Client records
- Communications with family members
- Conversations with partners and co-
- workers
- Sign in sheets
- Communications through an interpreter
- Treatment activity sheets/art work



HIPAA Overview

- DCAC is unique because it is sometimes difficult to determine who can access a client's PHI. In many cases, the person assigned as the legal guardian or representative for minor children can access the child's PHI.
- State law may provide exceptions to this rule such as when a minor is considered emancipated or if there is "reasonable belief" that the parent or personal representative may be abusing the child (45 C.F.R. 502(g)(5).
- DCAC may also have discretion to provide or deny parental access to the minor's record if a licensed health care professional makes a decision that such access could endanger the child.

HIPAA Overview

DCAC may not use or disclose PHI except as permitted or required by HIPAA Privacy Rule. The HIPAA PHI disclosure rules affect your day- to-day activities within a client service setting including talking to clients, talking with co- workers, computer work and making phone calls.

HIPAA Overview

Example: Phone Calls

When talking on the phone or in person, be sure the other person is allowed to receive the information. This is especially important to remember when taking phone calls. For example, a caller may pretend to be a family member to gain information that the client wishes to keep private. You must make sure the caller is really who he or she says they are before giving the caller information about the client. If at all possible, only limited information should be given over the phone.

HIPAA Overview

On her way to work in the Therapy Department, Lauren walks past two interns who are loudly discussing a client issue in a public area. Lauren knows the conversation is against DCAC's privacy policy. What should Lauren do?

A. Keep walking and ignore the interns. It's none of Lauren's business anyway.

B. Politely tell the interns that the client matter is private and should not be discussed in a public setting. Then report the incident to her supervisor, who should conduct an investigation and take steps to prevent similar incidents from occurring in the future.

C. Politely tell the interns the client matter private and should not be discussed in a public setting. Then hurry to the break room to tell her co-worker all about the incident.

HIPAA Overview

The answer is:

B. Politely tell the interns that the client matter is private and should not be discussed in a public setting. Then report the incident to her supervisor, who should conduct an investigation and take steps to prevent similar incidents from occurring in the future.

Discussion:

Private health information is being disclosed in a public area. Responsibility to immediately correct this behavior belongs to everyone. Corrective instruction should be offered to students, volunteers and employees alike. Supervisors will then address the matter further if necessary.

HIPAA Overview

HIPAA requires workers to use and share only the smallest amount of client information needed (minimum necessary) to complete many of their jobs. This means that representatives of the organization:

- Disclose only parts of client's record needed to complete the task.
- Identify which members of it's work force require certain PHI and limit access accordingly.
- Use standard protocols for recurring requests.
- Develop criteria to limit disclosures of PHI.
- Review requests on non-recurring disclosures on an individual basis under the criteria.

HIPAA Overview

However, the "minimum necessary requirement" does not apply to requests to or by a provider for uses and disclosures:

- For treatment
- Made to a client
- With the client’s authorization
- As required by law
- For The Department of Health and Human Services (HHS) for HIPAA compliance purposes.

It is important that you do not take advantage of your ability to access PHI. For instance, you should not look at the record of a family member, friend or neighbor for personal reasons.

HIPAA Overview

HIPAA requires that a covered entity provide a copy of its Notice of Privacy Practices (consent for treatment) to each client. The privacy notice identifies how DCAC may use and disclose PHI. It also presents the rights that clients have related to this information.

Key elements of the privacy notice include:

- A statement that the organization is required by law to maintain the privacy of PHI and to provide individuals with a notice of it's legal duties and privacy with respect to PHI.
- The name or title and phone number of a person or office to contact for further information.
- The date on which the notice is first in effect, no earlier than the date it is available.
- Be written in plain language.
- Include the client's rights with respect to PHI and a
- brief description of how the client may exercise rights.
- A description of all other purposes for which the organization is permitted or required to use or disclose PHI without the individual's direct authorization.

HIPAA Overview

Clients are guaranteed certain rights related to their health information and how that information is used.

- A client has the right to receive private communications in a certain way or at a certain place.
- A client has a right to look at and receive a copy of his/her PHI.
- A client has the right to amend PHI.
- A client has the right to receive an accounting of disclosures of PHI.
- A client has the right to receive a paper copy of the privacy.

HIPAA Overview

What you need to know about distributing the HIPAA privacy notice?

- Make a good faith effort to obtain an acknowledgement of receipt no later than the first service delivery date.
- The information should be posted in a prominent location and made available on the website where information about services is located.
- Updated HIPAA notices should be made available on or immediately after the date of any significant change.
- Employees must document client’s receipt of the notice.

HIPAA Overview

Fax machines should not be in areas accessible to the public. Faxing documents is a risk to confidentiality.

Carefully enter the number to ensure that the fax goes to the intended recipient. It is important to follow proper policies and procedures when faxing protected information.

HIPAA Overview

Never leave printed information out in the open for unauthorized viewing.

HIPAA Overview

When at a computer make sure the monitor is out of view of unauthorized users, especially the public. Never leave an electronic device *(DCAC laptop, desktop or iPad)* without logging off!

HIPAA Overview

- Safeguarding your password is one of the more important things you can do to protect PHI! Never leave your password written down and near your computer.
- Creating a password that can be easily guessed or recreated by others and sharing computer passwords threaten the security of client information.

HIPAA Overview

ADMINISTRATIVE CONTROLS:

Policies and procedures communicate DCAC's intent and commitment to information confidentiality and protection. Below is a description of HIPAA related policies and procedures that affect you.

- Department and Agency Manuals: describe the kinds of client information that employees need access to in order to do their jobs and practices related to authorized information disclosures.
- Information Technology Practices: limit access to client information
- for certain employee groups.
- Client Data Base (ETO) Procedures: provide a service desk to report suspected threats to client information such as viruses, problems with logins and privacy disclosures.
- Training Plans: educate employees about privacy and security on an ongoing basis.

HIPAA Overview

PHYSICAL CONTROLS: There are many ways to physically safeguard client information.

- Protect servers, routers and other equipment from damage, theft and misuse. Limit access to authorized staff members only, and lock up anything containing confidential information when not in use.
- Secure DVD's, flash drives and other portable electronic data as well as portable remote devices such as laptops, cell phones with e-mail capability through password protection and/or encryption.
- Reconfigure or write over confidential information to ensure that it is unrecoverable if deleting information. Deleting a file from a portable storage device, DVD or hard drive does not remove the information.

HIPAA Overview

TECHNICAL CONTROLS:

- Access to systems and information is based upon an individual's job function and "need to know".
- Computer viruses can seriously damage work stations, networks and information. Use caution when visiting websites or using media from an unfamiliar source. Installing unapproved software could infect your computer with malicious programs or unwanted spyware. If you encounter a virus on the computer you are using, contact your supervisor or seek IT support immediately.
- Firewalls protect computer systems from entry by unauthorized people.

HIPAA Overview

SOCIAL MEDIA

As DCAC employees, your personal use of social media may pose unintended risks to client privacy and proprietary information, reputation and brands and can jeopardize the agency's compliance with business rules and laws. Some general rules to follow include:

- Do not post or tweet information about clients or their families. There is a risk that identification of the client or family may occur even if the post appears to be unidentified.
- Do not post children's art work or materials created by clients on social medial/public sites.
- Do not accept requests to become a "friend" with a client or family member.

HIPAA Overview

In 2009, the Health Information Technology for Economic and Clinical Health Act, modified HIPAA to:

- require client notification, local media and HHS notification if certain PHI security breaches occur.
- hold business associates directly responsible for HIPAA compliance, subjecting them to civil and criminal penalties for wrongful disclosures of PHI.
- allow clients to restrict PHI among covered entities.

HIPAA Overview

Everyone at DCAC is responsible for information security. Any person who does business with or on behalf of DCAC as an employee, contract employee, student or volunteer must:

- Understand the reasons to maintain privacy and security of PHI and agree to abide by confidentiality policies and procedures.
- Keep client information confidential at all times- including all
- forms of communication: electronic, written and verbal.
- Report to your manager or information security leaders suspected or known violations of privacy and security.

Acknowledgement of Policy Manual

- I acknowledge receiving and reading the policy manual for Volunteers of Dallas Children's Advocacy Center related to HIPAA, Diversity and Inclusion, and Code of Ethical Conduct.
- As a Volunteer of DCAC, I understand that I am obligated to read this manual to familiarize myself with DCAC's expectations in regards to volunteering at the Center. Relatedly, I agree to abide by and adhere to all of these policies contained therein. If I do not understand any information in this manual, I agree to see clarification from my supervisor or the DCAC's Human Resources personnel.

Full Name: Date:

Enter your full name to confirm the above. Once complete, email this form to volunteer@dcac.org.