

Training Objectives

As a result of participating in this segment of training, learners will be able to:

1. Give a definition for HIPAA
2. List at least 5 pieces of protected information that can be used to identify a person
3. Summarize what to do in 3 out of 4 situations to safeguard communication and information (verbal, written, or electronic)
4. Explain “need to know” concept related to HIPAA
5. Describe how to use release of information and consent forms
6. Identify a guardian’s duties regarding protected health information
7. Classify the methods through which Protected Health Information can be transferred
8. Identify penalties for violation of HIPAA policy whether intentional or accidental

Estimated Time

1.5 hours, depending on the number of participants

Supplies

Laptop or computer connected to a projector/monitor

External speakers for laptop or computer

Internet access








Access to this Chapter’s visual content (including videos) on the DSHS website










Paper and pens for participants

Scratch paper








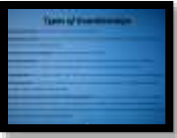

Print copies of your agency’s HIPAA Policy for handouts (or use the Sample Policy at the end of this chapter in this Trainer’s Guide)








Direct Support Professional Curriculum Toolkit







<p>Preparation before training</p>		<p>Review the Facilitator Guide for this chapter, and have enough Direct Support Professional Curriculum Toolkits for participants. Ensure each participant has a pen. And be sure to have reviewed the visuals and be prepared to ask the right questions following each brief video.</p>
<p>Opening: Engaging Activity (5 minutes)</p>		
<p>Say</p> 		<p>Now I would like each of you to write on a scratch piece of paper 3 things about yourself, and then turn the paper over in front of you.</p>
<p>Activity</p>		<p>Please write down:</p> <ul style="list-style-type: none"> • Your weight • Your bank balance • Time and description of your last bowel movement <p>Keeping the paper face down, slide it in front of the person to your right.</p>
<p>Note</p>		<p>Note to Facilitator: Pause for 15 seconds to make sure everyone has passed their face down paper.</p>
<p>Ask</p>		<p>Then ask participants to NOT look at the information, and to ask the person whose information they have, “Would you prefer to have your personal information posted on Twitter, Facebook, or would you like to have it back?”</p> <p>Encourage everyone to give the information back to the owner, unseen.</p>
<p>Reflection (1 minute)</p>		
<p>Ask</p> 		<p>How would you feel had that information actually been posted to that social media site? What would you want to happen to that person who posted it? We must be mindful of the HIPAA law, and of protecting people’s dignity.</p>
<p>Teach and Train (10 minutes)</p>		



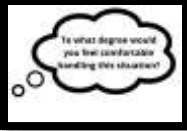





<p>Ask</p>		<p>What does the HIPAA acronym mean?! Gather guesses (it may be helpful to restate ideas shared).</p>
<p>Activity</p> 		<p>Then on the whiteboard or flipchart paper, write</p> <p>H I P A A</p> <p>with the corresponding words: Health Insurance Portability and Accountability Act.</p>
<p>Curriculum Toolkit</p>		<p>See Curriculum Toolkit for this chapter.</p>
<p>Ask</p> 		<p>While we may not use these terms, we DO need to know what it means.</p> <p>How many of us (raise your hand) have completed a HIPAA Acknowledgement Form at a doctor's office?</p> <p>What kind of information is considered protected, identifiable health information? Share your ideas and we'll capture them on the _____ (whiteboard or flipchart).</p>
<p>Activity</p>		<p>Write on the board/flipchart all of the types of information that participants share.</p>
<p>Curriculum Toolkit</p> <p>Note</p>	 	<p>Invite participants to turn to the My Notes section in the Curriculum Toolkit.</p> <p>Note to Facilitator: Be sure to circle these items on the board (from the ideas shared by those in the workshop). Have participants copy these items onto their HIPAA handout page in the Curriculum Toolkit. Types of Confidentiality / HIPAA Information:</p> <ul style="list-style-type: none"> • Name • Any location identifier more specific than state (address, zip code, city) • Social Security Number • Birth Date • Photograph








		<ul style="list-style-type: none"> • Case File • Email Address • Vehicle Identifiers (This refers to signage on cars that people ride in as well as t-shirts that label the person as having a disability by association of being with the person who wears it.) • Telephone Number <p>Be sure to share or add info on the board that may have not been included from the group:</p> <ul style="list-style-type: none"> • Any medical information • The fact that you work to support this individual • Financial status or payment details • Details of the day <p>Be sure to address the facts that:</p> <ol style="list-style-type: none"> 1. Initials are not protected information and may be used. 2. It is acceptable to speak in specifics about protected information to healthcare providers who support the same individuals or to supervisors and to some state agencies (licensor, auditor, or DDA Headquarters when asking for information). 3. It is also acceptable to share protected information when reporting incidents of abuse, neglect or domestic violence. <p>Written information that needs to be discarded must be handled appropriately; this may include shredding or filing/archiving in a secure location.</p>
<p>Ask</p>	<p style="text-align: center; font-size: 2em;">?</p>	<p>When it comes to the 3 types of information you were asked to write down at the beginning of this session: Weight, Bank Balance, and Bowel Movement, who might legitimately need to know this information about you?</p> <p>What types of information would a Direct Support Professional need to know in this role?</p>








<p>Activity</p> 		<p>Locate your agency's HIPAA Policy (your agency has one!), or make copies of the SAMPLE HIPAA Policy.</p> <p>HIPAA Policies include information about the Minimum Necessary (disclosure or rule) or Need to Know.</p> <p>Discuss what is needed to know in order to provide a service. Example, the bank will need to know your bank balance, but they do not need to know your weight.</p>
<p>Ask</p>		<p>What are the possible consequences of failing to follow HIPAA Policy?</p> <p>Review your agency's HIPAA Policy (or hand out and review copies that you made of the Sample Policy provided at the end of this chapter's Facilitator Guide).</p>
<p>Show</p>  <p>Ask</p> 	 	<p>Show <i>The Demanding Guardian</i> video (1:00) wanting personal information by phone.</p> <p>What should you do? What types of Guardians are there? What is a Release of Information? Answer: See below and the Curriculum Toolkit for this Chapter</p>
<p>Ask</p> 		<p>How do you know what information you can share? What type of information could that guardian receive? What types of guardians are there?</p>

<p>Curriculum Toolkit</p>		<p>Invite participants to review the sample Release of Information form found in this chapter of the Curriculum Toolkit.</p>
<p>Teach & Train (25-30 minutes)</p>		
<p>Say</p>		<p>Let's take a look at some potential, real-work situations where your knowledge of confidentiality is needed.</p> <p>Picture taking or videotaping by Direct Support Professional for personal use is prohibited (e.g., cell phones, social networking platforms, etc.). Use of pictures or videotaping for agency purposes requires signed consent.</p>
<p>Note</p>		<p>Note to Facilitator: Show the series of short video clips described below, stopping after each at the PAUSE & QUESTION slide. Allow staff to apply their learning to these real-work scenarios regarding confidentiality. Invite participants to relate how they should handle the scenario.</p> <p>Before showing the video, ask 2 participants to read one of the two roles shown in the video: Blue Box Person Gray Box Person</p>
<p>Show</p> 		<p>Show <i>Trip to Disneyland</i> video (0:37)</p>
<p>Ask</p> 		<p>You take a trip to Disneyland with the individual you support. Is it ok to put the pictures on your Facebook page? Why or why not? Answer: No, it is not ok to use individual photos for personal use.</p> <p>Explain how social media can be used in your role as a Direct Support Professional and that cannot be used.</p>

<p>Show</p> 		<p>Show <i>The Mall</i> video (0:27)</p>
<p>Ask</p> 		<p>While shopping with the individual you support, you run into a family friend of the individual. The friend asks questions about the individual’s health. Is it ok to answer the questions? Describe your responsibility as a staff in this situation.</p> <p>Answer: The individual can speak for themselves or the staff may disclose information if the individual has signed a consent for that friend. Things you may want to ask yourself include: Is there a confidentiality agreement? Do they “need” to know?</p>
<p>Curriculum Toolkit</p>		<p>Invite participants to review the <i>Your Responsibility</i> in the Fundamentals section Curriculum Toolkit while you discuss as a large group.</p>
<p>Note</p>		<p>Note to Facilitator: Your responsibilities for maintaining confidentiality. You may want to convey some of the following concepts about the role of a DSP.</p> <p>It may sound something like: In your position, you will be privy to some very private information about the people you support. This includes medical and financial information, as well as historical and personal information. It is essential that you hold all of this information in strict confidence. This means that you cannot share any of this information with anyone outside of other employees working with the individual unless you have explicit written consent to do so.</p> <p>There are some entities, such as federal or state agencies, which may be an exception to this. To ensure that you are always in compliance, it is best for you to refer any requests to your supervisor.</p> <p>This also applies to sharing information with your friends or family. Remember, personal information regarding the people you support should not be shared.</p> <p>When discussing issues regarding an individual, please ensure that you do so in a private area and that you are aware of others who may be listening. Never discuss one individual’s information in front of another</p>

		individual, even if you do not believe they are still listening or that they cannot understand.
<p>Show</p> 		Show <i>The Roommate</i> video (1:09)
<p>Ask</p> 		<p>While working in a home where several individuals live, an individual’s guardian stops by to visit. During the visit, the guardian asks questions about a roommate who lives in the home. Is it ok to answer the questions? To what degree would you be comfortable handling this situation?</p> <p>Answer: No, you may only speak about the individual the guardian represents.</p>
<p>Note</p>		<p>Note to Facilitator: While referring to the Your Responsibility in the Fundamentals section of the Curriculum Toolkit for this chapter may prove relevant based upon where the discussion goes with the group of participants, you may also want to bring up this information below as well.</p>
<p>Say</p>		<p>Maintaining confidentiality requires you to keep communication and information physically secure and in a secure area.</p> <p><u>Physically secure</u> means that access is restricted through physical means to authorized individuals only.</p> <p><u>Secured area</u> means an area to which only authorized representatives of the agency possessing the confidential information have access. Secured areas may include buildings, rooms, or locked storage containers—such as a filing cabinet within in a room—as long as access to the confidential information is not available to unauthorized personnel.</p>
<p>Show</p> 		Show <i>The Front Door</i> video (0:16)

<p>Say</p>		<p>The individual’s guardian arrives at the individual’s home demanding all paperwork regarding the individual.</p>
<p>Ask</p> 		<p>Do you give this information to them? What do you need to KNOW in order to handle this? Answer: Yes.</p>
<p>Show</p> 		<p>Show <i>Patio After Work</i> video (1:20)</p>
<p>Ask Note</p> 	 	<p>You are visiting after work with friends, including another employee from your agency. Is it ok to share your story of your day with your friends? Why or why not? Answer: No, it is not ok to discuss any information, even humorous stories, with someone who does or does not work directly with the individual.</p> <p>Note to Facilitator: Use the Curriculum Toolkit, notes earlier in this Facilitator Guide, and notes that participants may have taken during this session to use dialogue to close any learning gaps you perceive may exist with attendees. The <i>Teach and Train</i> emphasis in this session is reliant upon you as the trainer to facilitate “teaching” in a conversational manner following the video scenarios. Each class may go a little differently as participant input will vary.</p> <p>It is important that you train to meet each Objective in this chapter. By encouraging dialogue, you will make meaningful learning as staff put themselves in the staff shoes of the characters in the videos.</p>
<p>Reflection & Celebration (3-5 minutes)</p>		

<p>Ask</p> <p>Curriculum Toolkit</p>	 	<p>As a Direct Support Professional, what is your role to safeguard information? Responses may include;</p> <p>Refer to the 1, 2, 3, page in the Curriculum Toolkit as you reply</p> <ul style="list-style-type: none"> • Look for Release of Information in order to know what information may be shared with specific people • Share only pertinent information with people who have a need to know • Close the book/program when done documenting • Be thoughtful where I make med appointment calls, etc. • Do not discuss protected information about individuals you support outside of work (social media, family, friends, etc.).
<p>Activity</p>  		<p>Celebrate the privacy of personal information...invite all participants to SHRED the paper they wrote their weight, bank statement, or bowel movement information...as no one in the room needs to know! (Reinforce the appropriate discarding of information by shredding.)</p>
<p>Activity</p>		<p>Please administer the assessment at the end of this chapter.</p>
<p>Note</p>		<p>Note to Facilitator: Please review the objectives in the Curriculum Toolkit on the first page with participants. Ask participants to circle the objectives for this chapter in which they believe they need more clarity. Allow for question and answer dialogue to ensure that all of the objectives have been met.</p> <p>Hand out the assessment for this chapter to each participant. End of chapter assessments should take approximately 10 minutes.</p> <p>As a learning tool, it will be important for each participant to leave the training with the correct answers. Please review the answers and ensure that each participant has marked the correct answer. When you review the assessment with participants, note where people are having difficulty</p>

		<p>and review that section again with the whole group or determine where you will address this in the next chapter. Ensure that you reteach/retrain topics where learning gaps were identified.</p> <p>Due to the confidential nature of the assessments in this course, please collect and shred all completed assessments.</p>
--	--	--

Sample Agency HIPAA Policy Summary

The **Health Insurance Portability and Accountability Act (HIPAA)** is a federal law which was passed in 1996. HIPAA mandates that any “covered entity” and their employees must protect individually identifiable health information regarding a person’s physical or mental health as well as any healthcare that the person is receiving.

Under HIPAA, a covered entity refers to any health care providers, healthcare plan providers or healthcare clearinghouses that transfer healthcare data. We are trusted with a great deal of personal health and financial information for a large number of individuals. Disclosure of this information could result in a variety of issues from embarrassment and persecution to identity theft. It is our duty to protect the information of the people that we support as if it were our own.

HIPAA’s privacy rule protects all individually identifiable health information that is held or transmitted in any form, whether oral, paper, or electronic. Individually identifiable health information is defined as any information that relates to:

- i The individual’s past, present or future physical or mental health
- i Details of any healthcare that the individual is receiving or has received
- i Financial status or payment details

Also protected is any information that can be used to identify an individual including:

- i Name
- i Any location identifier more specific than state (address, zip code, city)
- i Social Security Number
- i Birth Date
- i Photograph
- i Case File
- i Email Address
- i Vehicle Identifiers
- i Telephone Number

Initials are **not** protected information and may be used. It is acceptable to speak in specifics about protected information to healthcare providers who support the same individuals or to supervisors. It is also acceptable to share protected information when reporting incidents of abuse, neglect or domestic violence.

This page left intentionally blank.

Protected information may also be disclosed to law enforcement representatives when there is a court order or when the information is important to the prevention or investigation of criminal activity. The only other time that protected information may be shared is when the disclosure is authorized in writing by the individual or their personal representative. A personal representative is described as a person who is legally authorized to make healthcare decisions on the individual's behalf.

A key provision of the HIPAA privacy rule is the "minimum necessary" disclosure. This means that any time a covered entity must disclose protected health information, the information shared is limited to the minimum necessary to accomplish the intended purpose of the disclosure, use, or request.

Privacy is extremely important when discussing any protected health information. A person overhearing a conversation in which protected health information is shared constitutes a violation of HIPAA. To prevent this, all discussions involving protected information should take place in a private setting such as in an office with a closed door. Having conversations in public or in a lobby area at work can cause unintended disclosure of protected health information. Avoid discussing any protected health information while not at work.

Protected health information in paper form must also be closely monitored to prevent viewing by any unauthorized entity. Be cautious when handling documents that contain protected health information and never leave them unattended. Also make sure that you are in a private setting before reviewing any documents that contain protected health information. Any paper documents which contain protected information must be shredded prior to disposal.

Security of electronic protected health information is also very important. Any employee who uses an electronic device for their job will select a password which will change every 90 days. Electronic devices should be angled so they are not readily noticeable to the public. Each computer has a screen saver that is activated after 10 minutes of disuse and will require a password to unlock. Anyone who uses an electronic device for work must also be wary of what they are downloading and what websites they are visiting. It is very easy to download a file which contains malware, or inadvertently click a link or to visit a website that will route to a site containing malware that can allow unauthorized entities to access our network or install key-logging software to copy passwords and any other information that is typed. Before disposing of any item that is used to store information, make sure that item is sanitized. If any device used for work purposes is stolen or misplaced, notify the security officer immediately so the device can be wiped remotely.

This page left intentionally blank.

As of September 23, 2013 the penalties for violation of HIPAA regulations increased. The new regulations establish four categories of violations and four corresponding levels of penalties depending on the gravity of the violation. The four categories of violations are:

- **Did Not Know:** Unintentional disclosure of protected health information
- **Reasonable Cause:** Accidental disclosure of protected health information due to a gap in training or communication
- **Willful Neglect Corrected:** HIPAA law is clearly ignored, but corrections are made to address the issue
- **Willful Neglect without Correction:** HIPAA law is clearly ignored and no corrections are made to address the issue

The table below will briefly outline monetary penalties:

Violation Type	Each Violation	Repeat Violations per year
Did not know	\$100 - \$50,000	\$1,500,000
Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
Willful Neglect Corrected	\$10,000 - \$50,000	\$1,500,000
Willful Neglect without Correction	\$50,000	\$1,500,000

Willful violations by individuals can also carry incarceration terms of up to 1 year per violation. Violations on either an individual or corporate level will also be reported the Secretary of the US Department of Health and Human Services and to media outlets.

HIPAA policy is enforced by three key positions within a company:

- **Chief Compliance Officer:** The Chief Compliance Officer oversees the compliance program as an independent and objective body that reviews and evaluates compliance issues or concerns within the organization
- **Privacy Officer:** Responsible for the development and implementation of the policies and procedures necessary for compliance. The Privacy Officer also receives complaints related to HIPAA.
- **Security Officer:** Responsible for developing appropriate policies to comply with the HIPAA security rule. Oversees and responds to any breach or impending breach of the security of Electronic Protected Health Information.