HIPAA – Safeguarding Protected Health Information

03/2021

WHAT IS HIPAA

HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA provides safeguards for PHI (protected health information) and rights for persons served. HIPAA privacy standards identify who has access to what PHI, persons' served rights of control over their health care information, defines inappropriate access and use of health care information, and determines who is accountable for protecting it.

WHAT IS THE PURPOSE OF HIPAA?

- HIPAA protects the privacy of the individuals we serve by establishing a national standard and guidelines for handling, storage and sharing protected health information.
- HIPAA allows individuals to make corrections in their own medical records.
- HIPAA allows individuals to know how personal information is shared and used.
- HIPAA gives individuals more control over who has access to their protected health information.

WHO IS REQUIRED TO FOLLOW HIPAA RULES?

The individuals that we support rely on our ability and willingness to maintain privacy and confidentiality while completing our job duties. Respecting their privacy is a crucial role for **ALL** Progress Industries employees.

What is PHI?

Protected health information, PHI, is any health information that can be connected to a specific person, including:

- Name
- Address
- Birthdate,
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record number
- Beneficiary numbers
- Account numbers
- License numbers
- Vehicle identifiers
- Device serial numbers
- Web URL's
- IP address numbers
- Fingerprints
- Full face photo images

Not all private information is PHI. For example, if you spoke only about a medical condition without identifying the person, you are not sharing PHI. Another example would be stating that you work as a DSP supporting people with disabilities. Because you have not mentioned anyone by name you have not disclosed PHI. However, if your statement mentioned the name of a person you supported, that, in combination with the fact that you work with people with disabilities would be an unauthorized disclosure. Be careful of identifiers and never release PHI without permission.

HOW ACCIDENTAL DISCLOSURE HAPPENS

One way that employees have unauthorized disclosures is when they **blog or post on social media.** Consider the following scenario depicting a Facebook post by a PI employee:

"I just love working for Progress Industries helping people with disabilities. The people I support are so much fun, especially Jacob. I think the reason we get along so well is that we have a lot in common. Even though he uses a wheelchair and can't speak, he really enjoys cars and music. We often go to the record store near his house on Grand Avenue."

Has this employee inappropriately shared PHI? Yes, because they used the person's name in combination with his disabilities and neighborhood where he lives. Watch out for OVERSHARING!

Another way employees can inappropriately disclose PHI is having conversations in public areas. Disclosure can be avoided by being aware of who may be able to hear your private conversations. Move to a private office or step outside and lower your voice.

Another way employees can accidentally share PHI is by sending emails or faxes to the wrong person. Make sure to double check email addresses and fax number before you send.

Additionally, leaving information in a common area such as a living room or kitchen, leaving file cabinets unlocked, throwing documents in the garbage instead of shredding them can also cause accidental disclosure.

And we can't forget information that is lost or stolen. This risk can be mitigated by keeping your phones and mobile devices password protected, securing information when you go into the community (medical cards, consultation forms, etc.) keeping devices hidden or secured in your trunk, and locking your vehicle.

Lastly, just because they are housemates, does not mean that you can share information about one person served with another, or their family or guardians. It is not an easy thing to do, but confidentiality among housemates is extremely important. We are not allowed to share ANY information about one housemate with another or their guardian/family members.

CONSEQUENCES OF COMPROMISED PHI

Individuals can be put at risk when PHI is compromised.

- They might experience **discrimination**. For example, if they have a communicable disease and the caregiver shares that information with others, they may refuse to work with that individual.
- If information is shared with a housemates' guardian or family members that puts them in a bad light, their **placement may be compromised**.
- They can become a victim of **identity theft.**
- If they feel they cannot trust providers to maintain their confidentiality, they may **avoid necessary treatment or services.**

HIPAA RULES

- Privacy Rule
- Security Rule
- Breach Notification Rule
- Enforcement Rule

The Privacy Rule

The Privacy Rule gives individuals more control over their PHI. The Privacy Rule sets national standards for how information can be used between professionals.

All employees of Progress Industries are responsible for knowing how to handle PHI appropriately. When sharing PHI you should follow the **Minimum Necessary Requirement** under the Privacy Rule. The requirement states that you should only share with other professionals the PHI necessary to complete a task or do your job, nothing more. DO NOT SHARE WITH HOUSEMATES' GUARDIANS OR FAMILY MEMBERS!

Consider the following scenario:

Jane works with a 23-year old man named Alex three times a week. She goes to his home where he lives with his mom, who is also Alex's conservator and plays a big role in Alex's care. Jane assists Alex with his medications, shopping, hygiene and grooming. One day Jane was helping Alex make out his grocery list. Alex was insistent that he wanted to buy some beer. Jane reminded him of the medication he is taking and that drinking alcohol is not a good idea. Alex replied, "it has nothing to do with my meds, it's just my Mom doesn't want me to have any fun. I can't wait until I move out of here." Upset about the beer, Alex refused to take his medications. At the grocery store Alex waved at a girl in the parking lot. Jane asked if he knew her. Alex replied, "yeah, she's kind of my girlfriend".

Applying the Minimum Necessary Rule, if you were Jane, what information would you share with Alex's mom?

- Alex's desire to purchase beer?

  No. This information is not essential for Alex's mom to know and he did not ask for it to be shared.

- Alex's comments about his mom and wanting to move out?

  No. This information is not essential for Alex's mom to know and he did not ask for it to be shared.

- Alex's refusal to take his medication?

  Yes. This information is essential for his mom to have as his caregiver.

- Alex's remark about having a girlfriend?

  No. This information is not essential for Alex's mom to know and he did not ask for it to be shared.

- WHAT can be shared?
- With WHOM?
- WHEN can it be shared?
- For what PURPOSE?
- Who can AUTHORIZE the sharing?

What can be shared?

You can share PHI with approval of the individual you support. At Progress Industries we utilize a form called a Release of Information that identifies what can be shared and who it can be shared with and for what time frame. When in doubt, review the release of information prior to sharing any PHI.

With Whom?

You may share PHI with other employees at Progress Industries who are involved in the support and care of the individual. With proper releases signed, you may share PHI with other community providers such as a primary care physician, psychiatrist, mental health professionals, and even family members.

When can it be shared?

Individuals have the right to limit the time frame in which information can be shared. It is best to review the release of information to determine that time frame. However, in situations where the individual may be incapacitated and requires emergency medical attention, you may disclose critical information necessary for Emergency Medical Technicians to provide care.

For what purpose?

You may need to share PHI for a variety of reasons. You may need to share information so that other professionals are able to provide treatment and support to the individual. The individual may need you to share information if they are trying to secure new services, housing, benefits, etc. The reason you share PHI must always be related to carrying out your job duties and support the individual.

Who can authorize sharing?

You are allowed to share information with other staff at PI who are directly involved in the person's care. Before you share information with people outside of PI you must have approval from the person or their legal representative. Check the signed release of information prior to sharing PHI.

The Security Rule

The Security Rule is a set of safeguards for electronic health information. Progress Industries must use these safeguards to protect information. We store and share PHI in electronic formats. The Security Rule has been updated to include specific requirements for protecting ePHI (electronic protected health information) that is shared or stored via email, internet, computers, or removable devices. The Security Rule outlines three distinct safeguards that we must use to protect ePHI.

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

You are responsible for understanding these safeguards.

Administrative Safeguards

Administrative safeguards are policies and procedures that are put in place to protect ePHI. For example:

- Designating a person in the organization to be the Privacy Officer
- Providing all staff with training about privacy
- Having policies in place that address access to PHI
- Having Business Associate Agreements with entities that may be able to access PHI

Physical Safeguards

Physical safeguards are measures that we take in our workplaces or anywhere that PHI is created, stored or shared. For example:

- Access to the building and offices within the building
- Securing email servers
- Having a disaster recovery plan to back up and restore PHI
- Having locked file cabinets
- Secure ways of destroying PHI (secure shred bins)

Technical Safeguards

Technical safeguards are ways that we can utilize technology to protect PHI. For example:

- Encrypting data
- Using Secure email
- Controlling access to PHI
- Creating user ID's and passwords for employees to access PHI
- Password protecting cell phones and removable devices

Safeguards that PI has in Place

- Meetings conducted in private areas.
- Telephones located in as private an area as possible.
- Documents are stored appropriately.
- Documents are not easily accessible to staff or visitors.
- Records are not left unattended.
- Records are protected from loss, damage and destruction.
- File rooms/cabinets are locked unless being used.
- Internal communications are enclosed in envelopes.
- PHI that is no longer needed is shredded prior to disposal.
- Temporary storage containers are labeled as confidential and emptied into the shred bins before leaving work each day.
- Any email sent from progressindustries.org to an external email is sent using P.I.'s encrypted electronic messaging system.
- Printers are located in areas not easily accessible.
- Computers require password for access.

The Breach Notification Rule

A breach is an unauthorized or accidental use of protected health information that compromises the security of PHI. If a breach occurs we are required to conduct a risk assessment and make a report. Not all unauthorized sharing of PHI is considered a breach under the Breach Notification Rule. In order for it to be a breach, there needs to be a threat that a person's PHI has been or will be compromised.

When protected health information (PHI) is shared without authorization, it is not automatically considered a breach. We must take steps to determine if a breach has occurred.

- **Step 1**: Report the Situation – If you are the person who discovers the problem you should contact the Privacy Officer of Progress Industries. Our Privacy Officer is Pam Eiler and she can be reached at 515-381-1936. No matter how small the incident, report it.

- **Step 2**: The Privacy Officer will initiate a risk assessment. During the assessment we will determine whether a breach has occurred, taking into consideration who had access to PHI, the identifiers shared, and whether or not PHI was actually acquired or viewed.

- **Step 3:** If we determine that a breach occurred it must be reported to the Department of Human Services and the individual(s) affected. If the breach involves more than 500 individuals we must also share it with the local media.

Examples of Possible Breaches that You Should Report to the Privacy Officer

- You faxed a document with PHI to the wrong fax number.
- After a meeting in the community you left behind files containing PHI.
- You sent an email with sensitive PHI to the wrong email address.
- Someone broke into your laptop where you store PHI for those you support.

The Enforcement Rule

The Enforcement Rule explains the consequences for failing to keep PHI safe. The federal government may make companies or employees pay hefty fines or be imprisoned. Often these punishments are given to people who share PHI on purpose for personal gain. As an employee of Progress Industries you should make it a priority to keep PHI of those you support safe and secure.