HIPAA and Fraud, Waste, & Abuse 2021-2022 Training

HIPAA

Health Insurance Portability and Accountability Act

TRAINING

Training Description

This training course is designed to provide an overview of state and federal rules, regulations, and laws that govern the Non-Emergency Transportation Management (NEMT) industry.

Employees, contractors, transportation providers, and drivers of Medi Trans are required to complete this training annually.

What's Covered

1. What is HIPAA?
2. Uses and Disclosures
3. Your Responsibility
4. HIPAA Compliance
5. Members' Rights

What You'll Learn

After completing this training, you will be able to:

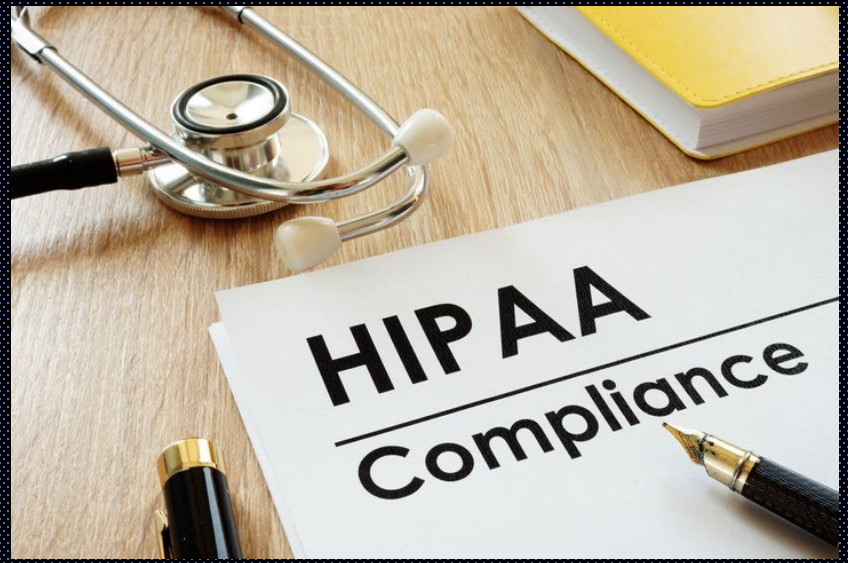
- Define the requirements of the Health Insurance Portability and Accountability Act (HIPAA).
- Identify Protected Health Information (PHI)
- Explain the uses and disclosure/release of PHI
- Recognize how HIPAA and PHI impact your role
- Understand what corrective actions or disciplinary actions may be taken for not complying with HIPAA
- Explain member's rights
- Perform your role in compliance with HIPAA

1. What is HIPAA?

HIPAA

The **Health Insurance Portability and Accountability Act (HIPAA)** is a federal law passed in 1996 due to the rapid growth of health information systems and the need to keep individuals' health information safe.

HIPAA includes many parts. This training will only review the parts that apply to our business.



The Privacy Rule

The **Privacy Rule** is core part of HIPAA.

It is a set of national standards put in place to protect certain health information.

The standards address the use and release of individuals' **Protected Health Information (PHI)** by organizations like Medi Trans.

Protected Health Information

The HIPAA Privacy Rule protects the privacy and confidentiality of information known as Protected Health Information (PHI).

PHI is health information that can be tied to a specific person and is:

- Transmitted electronically;
- Maintained electronically; or
- Transmitted or maintained in any other way.

Covered Entities & Business Associates

The **HIPAA Privacy Rule** applies to all **Covered Entities** and their **Business Associates.**

Covered Entities & Business Associates

Covered Entity

A healthcare provider, health plan, or healthcare clearing house that electronically transmits and receives PHI.

Business Associates

An entity or person who performs services or functions for a Covered Entity. The Privacy Rule allows a Covered Entity to share PHI with its Business Associates.

A Covered Entity must have a contract with their Business Associate, called a Business Associate Agreement. This agreement prevents Business Associates from using or releasing PHI in any way that would violate the Privacy Rule.

PHI Components

To be considered **PHI**, the information must have two components or parts:

Medical Information – information about a person's past, present, or future physical or mental healthcare received, or healthcare payment information.

Personally Identifiable Information (PII)– Pieces of data or information that can be used to identify a person.

PHI Components

Medical Information including past, present, and future:

- Health Condition
- Health Payment Information
- Mental Healthcare Received
- Physical Healthcare Received
- Healthcare Diagnosis
- Dates of Service
- Diagnosis Codes

PHI Components

Personally Identifiable Information (PII) includes:

- Name
- Dates (birth date, admit date, discharge date, etc.)
- Address
- Names of Relatives
- Name of Employer
- Telephone Number
- E-mail Addresses
- Social Security Number
- Medicaid/Medicare Number
- Member ID Number
- Medical Record Number
- Finger Prints
- Voice Recordings
- Photographic Images

Protect PHI

HIPAA protects all elements of Protected Health Information (PHI).

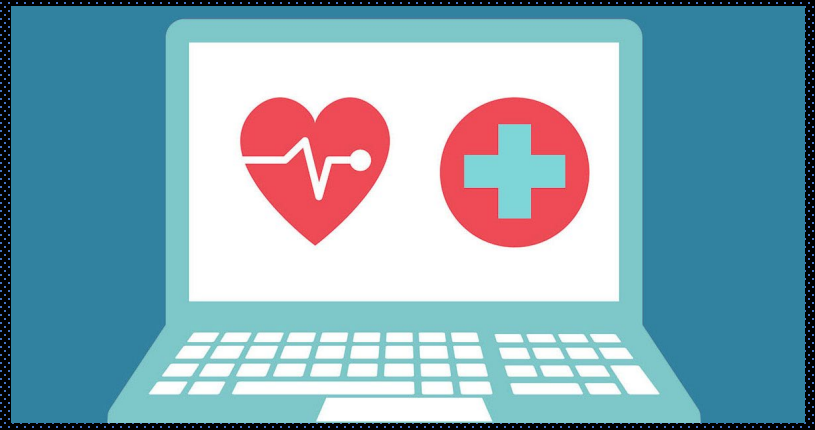
Improper access, use, or release of PHI is a violation of HIPAA and the Privacy Rule.

HITECH Act & the HIPAA Omnibus Rule

The **Health Information Technology for Economic and Clinical Health (HITECH) Act** was put into practice as part of the **American Recovery and Reinvestment Act (ARRA)** of 2009. This act encouraged the use of electronic health records (EHRs).

The use of EHRs has been shown to improve the quality, safety, and coordination of healthcare.

The **HIPAA Omnibus Rule** is a set of regulations that changed HIPAA's privacy, security, and enforcement rules to include various parts of the HITECH Act.



Breach

Breach – The access, use, or release of PHI in a way that is not allowed under HIPAA.

Breach Notification Rule

The **Breach Notification Rule** requires Covered Entities to notify affected individuals, The U.S. Department of Health and Human Services (HHS), and sometimes, the media when a breach of unsecured PHI occurs.

Individuals

HHS

2. Uses and Disclosures

PHI Use and Disclosure

The Privacy Rule tells us when a person's PHI can be used or released.

Use – To share, utilize, examine, or analyze PHI *within Medi Trans*

Disclosure – To release, transfer, or share PHI to an organization or person *outside of Medi Trans*

PHI Use and Disclosure

Example of Use: An associate at Medi Trans might look at the PHI of a member to decide whether they are eligible for transportation services.

Example of Disclosure: An associate at Medi Trans shares information with a transportation provider so they may safely transport a member.

Examples of PHI Violations

- Discussing a member's PHI with others who have no need to know (in person, on social media, by email, etc.)
- Leaving a member's information in places that can be accessed by others (on desks, seats, etc.)
- Selling or releasing medical information
- Throwing away printed materials that may contain personal information (these items must be shredded)
- Providing information to others without the permission of the member

Disciplinary Actions - Subcontractors

For Transportation Providers and other subcontractors, corrective actions that Medi Trans may take when HIPAA rules are broken are defined in our contract with your company, the Business Associate Agreement, and any other agreements between our organizations.

4. HIPAA Compliance

Human Resource Office

HIPAA regulations require that we designate a **Privacy Office / Officer** to perform specific privacy tasks.

The Privacy Office is operated by Medi Trans Director of Human Resources, in conjunction with our COO. This office oversees all activities related to developing, implementing and maintaining our organization's privacy policies according to federal and state laws that apply to our business.

Brittany St. Julien, Director of Human Resources.

Phone: 337.534.4484 ext. 105

Email: Privacy@CallMediTrans.com

Morgan Landry, COO.

Phone: 225.892.7488

Email: MLandry@CallMediTrans.com

Your Responsibilities

All associates, subcontractors, and vendors of Medi Trans are responsible for:

- Preventing access to or use of PHI that is not allowed by HIPAA.
- Watching out for illegal use or release of PHI.
- Reporting illegal use or release of PHI to your supervisor or to Medi Trans' Privacy Office.

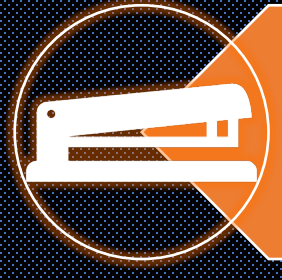
Protect a member's PHI as if it were yours!

Safeguarding PHI

Computer Security

Faxes

Email



Workspace

Instant Messaging

Public Areas

Safeguarding PHI

Computer Security

Your computer or mobile device are the main tools you use to perform your job. It is important to secure your primary tool/device.

- Never allow anyone to use your device.
- Never share your username or password with anyone.
- Never write down your password and leave it in a place that is not secure.
- Always lock your device before you step away from your workspace.
- If you use a laptop, make certain it is secured when leaving for the day.
- Always use a “strong password” as required by our security policies.

Safeguarding PHI

Email

Email is an important way to communicate but there are security risks you should be aware of when using email.

- You may not email or forward PHI to anyone unless it is needed to perform a specific task.
- You may not email PHI outside of Medi Trans unless you have permission.
- You may not email private information or PHI to personal email accounts.
- If you are allowed to send PHI outside of Medi Trans, you must do so by using the IT encryption process.
- If you do not understand the encryption process, ask your manager for extra training.

Safeguarding PHI

Instant Messaging

Instant messaging is an easy way to communicate. However, it is not secure!

Instant Messaging Guidelines:

- Do not chat about PHI through instant message.
- Do not send PHI or PHI-related documents through instant message.

Safeguarding PHI

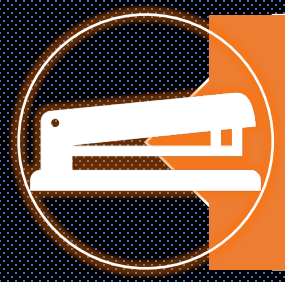
Faxes

At times, we send and receive faxed information as part of our daily work. PHI by fax is risky. For this reason, it is our policy to fax only when absolutely necessary.

Fax security guidelines:

- In the rare event that you are sending PHI by fax, you must use the standard cover sheet, which includes the Corporate “Confidentiality Statement”.
- Double-check that the fax number you are sending to is correct before sending.
- You must check the “sent” records for each fax that contains PHI, right after the transmission.
- **If you accidentally send PHI to the wrong place, you must report it to the Privacy Office right away.**

Safeguarding PHI



Workspace

Whether you work in a cubicle, office, a vehicle, or at home, PHI should be stored within locked rooms, drawers, cabinets, or containers.

Workspace security guidelines:

- Documents that contain PHI should never be left around your workspace at any given time.
- Paper documents containing PHI should be shredded when no longer needed.
- Any associate who is authorized to work from home should make sure that their home office complies with all applicable policies and procedures regarding the security and privacy of PHI.

Safeguarding PHI

Public Areas

You should always be aware of your surroundings when you have PHI in public areas such as the kitchen, elevator, corridors, a vehicle, etc.

Guidelines for protecting PHI in Public Areas:

- Avoid talking about members' PHI in public areas
- If talking about a members' PHI in a public place cannot be avoided, make sure that you do not use specific information that might identify a member
- When handling PHI in public areas, make sure others cannot see it and that all documents with PHI are secure before leaving the area

Common Privacy Mistakes

The most common privacy mistakes include:

- Leaving your ID badge visibly unattended
- Leaving private/protected health information out in the open and unsecured at your workspace and in public areas (copier/fax machines)
- Leaving keys to lockable cabinets and doors in the lock
- Leaving your computer unlocked and unattended
- Leaving portable company devices (laptop or mobile device) out in the open and unattended

5. Members' Rights

Members' Rights

Member Complaints:

- If a member thinks their privacy has been violated, they have the right to file a complaint.
  - Members may contact Member Services to file a complaint and the Privacy Office will investigate
  - Members may also file a complaint directly with the U.S. Department of Health and Human Services
- The HIPAA Privacy Rule prevents us from interfering with members' rights to complain and express their opinions about their PHI.
- We cannot ask members to give up their rights in order to receive service.
- We also may not intimidate, threaten, pressure, discriminate against, or retaliate in any way against members who file a complaint.

Members' Rights

Members have the right to:

Limit the use or release of their PHI

See the PHI we use to make decisions and make corrections if they see something wrong

Have us communicate their PHI in a special way

See all of their PHI that we may have released

MediTRANS

Fraud, Waste, & Abuse

Reducing Inappropriate and Wasteful Use of Federal Funds

TRAINING

Training Description

This training course is designed to provide an overview of state and federal rules, regulations, and laws that govern the Non-Emergency Transportation Management (NEMT) industry.

Employees, contractors, transportation providers, and drivers of Medi Trans are required to complete this training annually.

What We'll Cover

1. The False Claims Act (FCA) & Deficit Reduction Act (DRA)
2. The Fraud Enforcement & Recovery Act (FERA)
3. The Anti-Kickback Statutes (AKS)
4. The Physician Self-Referral Law (Stark Law)

What You'll Learn

When this training is finished, you will be able to:

- Define each of the following laws:
  - The Federal False Claims Act (FCA)
  - The Fraud Enforcement and Recovery Act (FERA)
  - The Deficit Reduction Act (DRA)
  - The Anti-Kickback Statute (AKS)
  - The Physician Self-Referral Law (Stark Law)
- Describe the benefits of each law and the punishments for breaking them.
- Understand that breaking any law may mean a person or company can no longer work or take part in federal healthcare programs. This includes Medicare and Medicaid.

1.

The False Claims Act (FCA) & Deficit Reduction Act (DRA)

Federal False Claims Act (FCA)

The Federal False Claims Act (FCA) protects the government from being overcharged or sold low quality goods or services.

The FCA holds any person responsible who knows or who has reason to think a claim is false, but submits it to the government for payment anyway.

Deficit Reduction Act (DRA)

The Deficit Reduction Act of 2005 (DRA) is used to reduce Medicaid fraud and abuse. The DRA applies to all healthcare providers receiving at least $5 million in payments from Medicaid every year.

False Claims Example

Example:

A transportation provider intentionally submits a claim for non-emergency transportation they know they **did not provide**. By doing so, this transportation provider has committed **fraud**.

Fraud resulting from false claims **costs the United States billions of dollars each year.**

Qui Tam (Whistleblower Provision)

An important part of the False Claims Act is known as **“qui tam”.** It allows any person or organization that has evidence of fraud against **federal programs or contracts to file a lawsuit on behalf of the U.S. Government.** The government has a right to participate in the lawsuit.

Those who file qui tam lawsuits are known as **“whistleblowers”.**

Whistleblower Incentive and Protection

Incentive:

Whistleblowers may be awarded a part of any money that is collected from a qui tam lawsuit.

Protection:

Medi Trans has a zero-tolerance policy for retaliation or retribution against any employee or subcontractor who in good faith reports suspected Fraud, Waste, & Abuse. Any employee found in violation of this policy will be subject to disciplinary action, up to termination of employment

Additionally, any employee who is fired, demoted, suspended, threatened, harassed, or discriminated against because they filed a qui tam lawsuit can seek double the amount of pay they would have received while fired, demoted, or suspended. They may also ask for other damages and fees.

Violation Penalties

Those who do not obey the False Claims Act must pay the federal government three times the amount of damages they caused the government, in addition to other possible punishments called civil penalties.

Civil penalties can range from $10,781 to $21,562 *per* violation.

In addition to monetary penalties, there may be additional restrictions like being **banned from working on or participating in federal and state government contracts.**

2.

The Fraud Enforcement & Recovery Act (FERA)

Fraud Enforcement & Recovery Act (FERA)

The **Fraud Enforcement and Recovery Act (FERA)** was signed into law in 2009.

FERA makes it easier for the government to investigate and punish those who violate the False Claims Act.

3. The Anti-Kickback Statutes (AKS)

Anti-Kickback Statute (AKS)

In 1972, Congress passed the first **Anti-Kickback** rules as a way to prevent fraud and outlaw dishonest behavior.

These rules say that it is a crime for individuals or companies to offer, pay for, ask for, or receive something of value in exchange for referrals of business under federal healthcare programs.

Example:

A transportation provider offers to pay customer service representatives to assign them more expensive trips.

Penalties of AKS

The Federal Anti-Kickback Statute is a criminal law and the punishment for violation of the law can be severe.

Punishments can include:

- Fines up to **$25,000** each time the law is broken
- A **felony conviction** with **jail time**, or both;
- The possibility of being **banned from working in or with** federal healthcare programs

4. The Physician Self-Referral Law (Stark Law)

Physician Self-Referral Law (Stark Law)

Physician self-referral is the practice of a doctor sending a patient to a medical facility that is owned by the doctor or the doctor's family member.

The Stark Law makes it illegal for a doctor to do this.

The main reason for the Stark Law is to make sure that money or profits do not cause incorrect medical decisions on the part of doctors and other healthcare workers.

Stark Law Penalties

Punishments for breaking the Stark Law include:

- **Denial of payment** from Medicare or Medicaid for health services that violated the law
- Any **payment** received for an illegal referral **must be returned**
- Up to **$15,000 fine** for each service provided while breaking the law
- Up to **$100,000 fine** for taking part in a scheme that breaks the law
- **Being banned** from the **Medicare and Medicaid** programs

FWA Compliance Office

It is your responsibility to report and suspected Fraud, Waste, or Abuse to MediTrans FWA Compliance Office. Your report is strictly confidential and cannot be use against you in any way.

The FWA Compliance Office is operated by Medi Trans Director of Human Resources, in conjunction with our DOO. This office oversees all activities related to developing, implementing and maintaining our organization's FWA policies according to federal and state laws that apply to our business.

Brittany St. Julien, Director of Human Resources.

Phone: 337.534.4484 ext. 105

Email: Fraud@CallMediTrans.com

Jon Lester, DOO.

Phone: 337.346.3106

Email: JLester@CallMediTrans.com

MediTRANS

Assessment and Attestation

Let's see what you learned by clicking here