VERIDA

Annual Compliance Training - Driver

2023-2024

Training Overview

This course is designed to provide an overview of accreditation requirements, as well as state and federal rules, regulations, and laws that govern the Non-Emergency Transportation Management (NEMT) industry. It also covers Verida's Code of Conduct, and the Company’s expectation of ethical behavior in all that we do.

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

VERIDA

HIPAA -

Health Insurance Portability and Accountability Act

What We'll Cover

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 members' 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 a 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 Verida.

Protected Health Information (PHI)

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.

Protected Health Information

Covered Entity

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.

Covered Entities & Business Associates

Business Associate

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.

Covered Entities & Business Associates

To be considered **PHI**, the information must have two 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 specific 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
- Fingerprints
- Voice Recordings
- Photographic Images

PHI Components

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

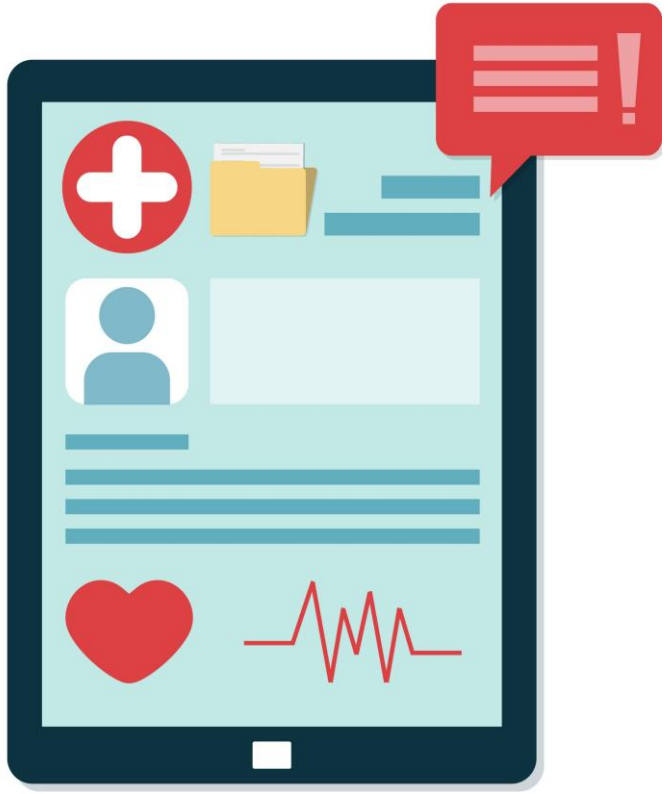
Improper access, use, or release of PHI is a violation of HIPAA and the Privacy Rule.

HITECH Act & 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

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 impacted individuals, the U.S. Department of Health and Human Services (HHS), and sometimes, the media when a breach of unsecured PHI occurs.

Individuals

HHS

Media

Breach Notification Rule

Individuals

Individuals who are affected by a breach must be notified no later than 60 days from the time of discovery.

Media

The **Media** must be notified of a breach involving 500 or more individuals. The notification must occur no later than 60 days from discovery.

Breach Notification Rule

HHS

The U.S. Department of Health and Human Services (HHS) requires healthcare companies to submit a log of all breaches involving fewer than 500 individuals once a year, no later than 60 days after the end of the calendar year.

A breach that involves 500 or more individuals must be reported to HHS no later than 60 days from the time of discovery.

2. Uses & Disclosures

PHI Use & 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 Verida*.

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

PHI Use & Disclosure

Example of <u>Use</u>: An associate at Verida might look at the PHI of a member to decide whether they are eligible for transportation services.

Example of <u>Disclosure</u>: An associate at Verida 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 member's permission

3. Your Responsibility

HIPAA & You

Verida and you, as an associate, are expected and required to follow all standards and regulations set forth under HIPAA.

Minimum Necessary Rule

The Minimum Necessary Rule restricts the use and disclosure of PHI to only the minimum amount needed to complete specific tasks.

Here are some guidelines:

- Look at PHI only if your task requires it.
- Use only the minimum amount of PHI needed to complete your task.
- Talk to others about PHI only if it is necessary to perform your task.
- Give PHI to others only when it is necessary to perform their task.

Administrative Procedures

The Minimum Necessary Rule impacts administrative procedures, workflows, and information systems.

Verida has taken steps to implement this standard, especially in the following areas:

- Routine and Recurring Requests: such as reports required by agencies like Medicaid
- Assignment of Access Profiles: to determine what information you may access through your computer, based on your job description
- Limited Data Sets: very limited information provided for approved research, public health, or healthcare operations only

Disciplinary Actions - Associates

Verida takes violation of privacy rights very seriously. If one of our associates deliberately violates privacy polices and procedures, they will be subject to the Verida disciplinary process outlined in the Employee Handbook.

Disciplinary Actions - Subcontractors

For Transportation Providers and other subcontractors, corrective and progressive actions that Verida may take are further defined within the contract, Business Associate Agreement, or other agreements between the parties.

4. HIPAA Compliance

Privacy Officer

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

The Privacy Officer 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.

Jason Henderson is our Privacy/Security Officer.

Privacy Line: (470) 240-5392

Privacy Email: security@verida.com

Privacy Policy & Procedure Maintenance

Verida is responsible for being up to date on all HIPAA rules and regulations.

If the Privacy Rule changes significantly in the future, Verida will update our policies and procedures to comply with the new regulations. All associates will be re-trained on any changes that affect their jobs.

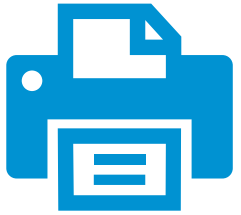
Your Responsibilities

All Verida associates, subcontractors, and vendors 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 Verida's Privacy Officer

Safeguarding PHI

Computer Security



Faxes

Email

Workspace

Instant Messaging

Public Areas

Safeguarding PHI

Computer Security

Your computer, tablet, or phone is the main tool 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.
- Always secure your laptop/desktop 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 the company unless you have permission.
- You may not email private information or PHI to personal email accounts.
- If you are authorized to send PHI outside of the company, 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

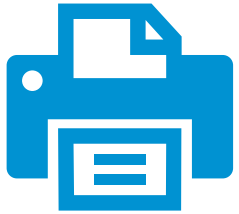
Instant Messaging

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

We send and receive faxed information as part of our daily work but sending PHI by fax is risky! It is our policy to fax only when necessary.

Fax security guidelines:

- In the rare event that you are sending PHI by fax, be sure to use the standard cover sheet with the Corporate “Confidentiality Statement”.
- Double-check that the fax number you are sending to is correct.
- 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 Officer 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 time.
- Paper documents containing PHI should be shredded when no longer needed.
- Any associate who is authorized to work from home should make sure their home office complies with all company 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 member's 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, iPad, or mobile phone) out in the open and unattended

5. Member Rights

Member Rights

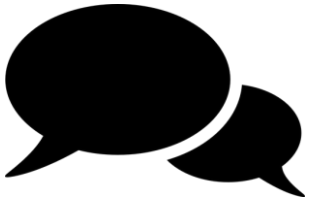
- If a member thinks their privacy has been violated, they have the right to file a complaint. Member may:
  - Contact Member Services to file a complaint and the Privacy Officer will investigate
  - File a complaint directly with the U.S. Department of Health and Human Services
- The HIPAA Privacy Rule 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.

Member 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 their PHI that we may have released

VERIDA

Compliance Laws & Fraud, Waste, and Abuse

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)
5. Verida's Fraud, Waste, & Abuse Program

What You'll Learn

After completing this training, you will be able to:

Define each of the following laws:

- The Federal False Claims Act (FCA)
- The Deficit Reduction Act (DRA)
- The Fraud Enforcement and Recovery Act (FERA)
- 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.

False Claim 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**.

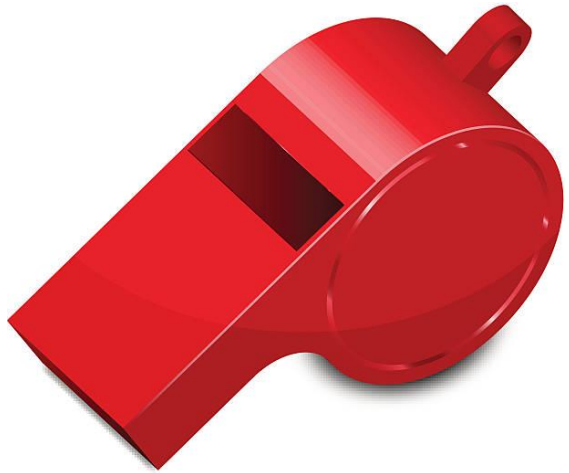
Fraud resulting from false claims **costs the United States billions of dollars each year.**

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.

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 & Protection

Incentive:

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

Protection:

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.

False Claims Act Cases

In 2022, the U.S. Department of Justice recovered more than $2.2 billion in civil FCA judgments and settlements.

Of the $2.2 billion in settlements and judgments, over $1.7 billion related to matters that involved the health care industry, including drug and medical device manufacturers, managed care providers, hospitals, pharmacies, hospice organizations, laboratories, and physicians.

Violation Penalties

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

Civil penalties currently range from $13,508 to $27,018 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)

The Fraud Enforcement & Recovery Act

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 Statute (AKS)

The AKS Rules

In 1972, Congress passed the first **Anti-Kickback** rules 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, including Medicaid and Medicare.

Example:

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

Purpose of Anti-Kickback Statute

The primary function of the Anti-Kickback Statute is to **make certain that financial motives do not undermine the integrity of the medical judgment** that must be maintained by physicians and other health care and health care related service providers.

The Anti-Kickback Statute promotes referrals to individuals or groups for health care services based on medical need rather than financial or other types of incentives.

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 **$100,000** each time the law is broken
- A **felony conviction** with up to **10 years of jail time**, or both
- The possibility of being **banned from working in or with** federal and state healthcare programs

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

Physician Self Referral

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**
- If found guilty of a violation, fines may be enforced up to **$100,000** for each violation
- A prison term for up to **five years**
- **Being banned** from the **Medicare and Medicaid** programs

5. Verida's Fraud, Waste, & Abuse Program

Fraud, Waste, & Abuse Defined

What is Fraud?

Fraud is wrongful or criminal deception intended to result in financial or personal gain. Examples include:

- Wrongful administration of Medicaid/MCO programs
- Provider or member fraud and abuse
- Billing for services not provided
- Submitting false claims
- Theft or taking financial advantage
- Kickbacks (Anti-kickback Statute and The Stark Law)
- Up-coding or over billing for services, and
- Drug diversion

Fraud, Waste, & Abuse Defined

What is Waste?

Waste may relate primarily to mismanagement, inappropriate actions, and inadequate oversight.

Example: *Providing services that are not medically necessary.*

What is Abuse?

Abuse includes practices that result in unnecessary costs to government programs, such as:

- Faulty financial, business, or medical practices
- Seeking payment for goods or services that are not medically necessary or do not meet the recognized standards for health care.

Fraud, Waste, & Abuse Defined

Failure to report suspected fraud can be grounds for termination and even criminal prosecution. Report suspected fraud in the following ways:

Verida Compliance
Chris Lee, Chief Compliance Officer
Compliance Hotline: (855) 299-9309
clee@verida.com or
corpcompliance@verida.com

Verida Internal Audit
Internal Audit Line: (404) 942-4278
reportfraud@verida.com

Medicaid Fraud Control Unit (MFCU)
Provider Fraud or Abuse
Call toll-free: 1-800-433-5454

Office of Inspector General (OIG)
Call toll-free: 1-800-433-3982