



# VSP Vision Annual Privacy Training



*brought to you by VSP Vision Office of the General Counsel*

In the digital age we live in, where most personal information is stored and exchanged electronically, the demand for data privacy and protection safeguards is more important than ever. As such, protecting VSP Vision® (VSP) data from all kinds of loss, theft, or misuse is the responsibility of each VSP workforce member.

This privacy training is required for any VSP Vision contractor, employee, or affiliate who accesses, processes, or handles PII/PHI on behalf of VSP. This training will explain your role in protecting personal data from internal and external threats.


## **At the end of this course, you will understand:**

- The importance of privacy at VSP.
- The different kinds of data that VSP manages.
- Key data privacy laws and related rights.
- The consequences of privacy violations.
- The Fair Information Principles.
- How to recognize and report unauthorized disclosures.


- When to complete a Privacy Impact Assessment (PIA).
- Your responsibilities related to privacy at VSP.

We estimate this course will take about 30 minutes.


 **What is Data Privacy?**


 **Quiz Break #1**


 **Data Privacy Laws**

 **Quiz Break #2**

 **Privacy Impact Assessments**

 **Quiz Break #3**

 **Identifying, Reporting, and Preventing Privacy Incidents**

 **Quiz Break #4**

 **Training Conclusion**

# What is Data Privacy?

---



---

Before we dive in, let's examine what privacy is and why it's so important at VSP.

Flip the cards below to proceed.

What is Privacy?

Defined broadly, privacy is the right of an individual to determine for themselves when, how, and for what purpose their personal information is handled by others.

Why Does Privacy Matter?

Protecting the privacy of our members, consumers, fellow employees, and business partners is key to ensuring dignity, safety, and the right to be free from discrimination.

Why is Privacy Important at VSP?

Privacy is a way VSP demonstrates respect and value for our members and consumers. If they feel VSP is not taking their privacy seriously, it can lead to litigation, penalties, and the potential loss of business.

## Different Types of Data

As a regular part of doing business, VSP collects many different types of personal information about our audiences, including members, consumers, doctors, clients, brokers, business partners, and employees.

Personal information, sometimes referred to as **Personally Identifiable Information (PII)** is data, whether on its own or in combination with other data elements, that can be linked to a single individual. For example, something like a person's name or Social Security number is a clear instance of PII. Less obvious examples might include an IP address, email address, credit card number, or pictures of faces.

PII can also include odd combinations of unidentifiable information. For example, if you combine ZIP code, education history, veteran status, and first name, you would likely be able to identify the individual. For this reason, there is no comprehensive list of data fields for personal data.

## Let's explore the different types of PII

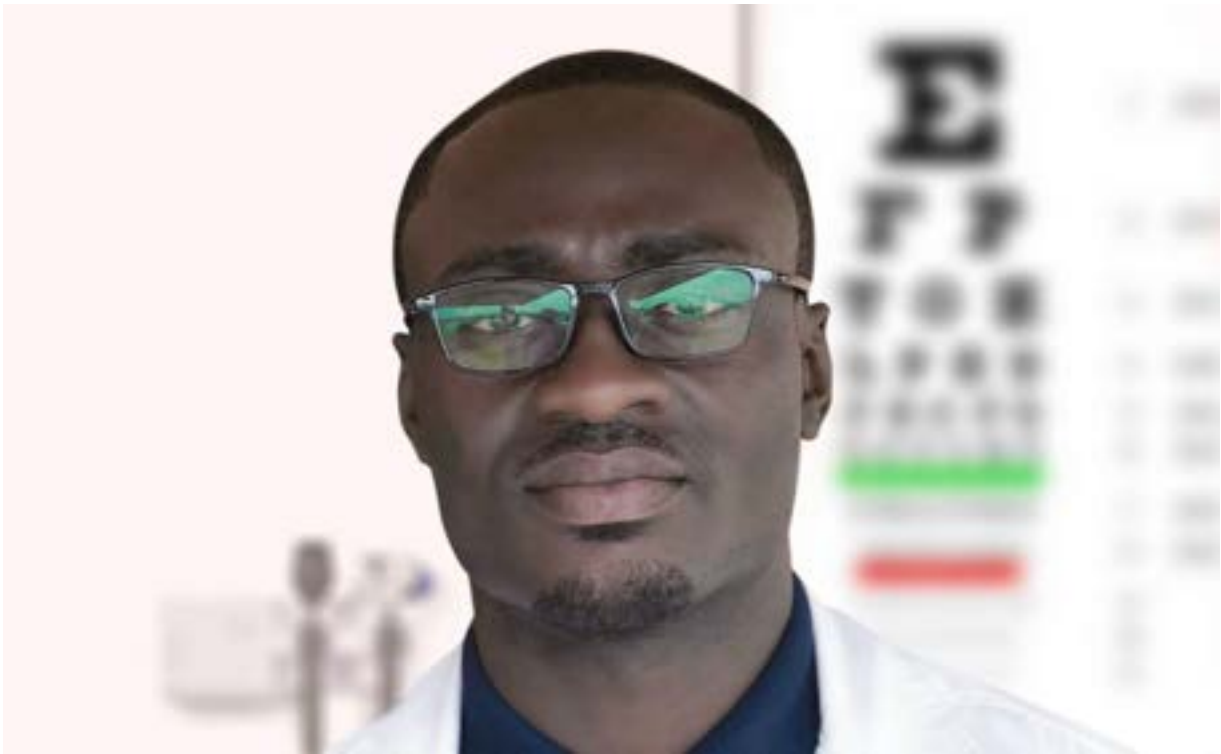
## Protected Health Information (PHI) —

One subset of PII is PHI. PHI is defined as data in any form (electronic, written, or verbal) that identifies an individual AND which relates to that person's past, present or future health, healthcare, or payment for healthcare.

Health information may include:

- Member/patient identification number
- Dates - including birth, discharge, admittance, and death dates
- Medical notes of symptoms or diagnosis
- Test results
- Prescription information
- Provider information/location

PHI, because of its sensitivity, is highly regulated, and all VSP employees should use extra caution when accessing or handling it.



## Sensitive Personal Information (SPI) —

SPI is data that includes sets of “special categories” that must be treated with extra security. These special categories are typically ones that could be used to discriminate against individuals. This includes information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Data related to a person’s sex life or sexual orientation
- Biometric data – fingerprints, facial recognition, etc. (where processed to uniquely identify someone)



## Payment Card Information (PCI) —

Our final subset of PII is PCI. PCI refers to credit card information and applies to all merchants and vendors that handle card data, including those that accept, or process payments made through printed forms, over the phone, in person or online.

This type of data includes:

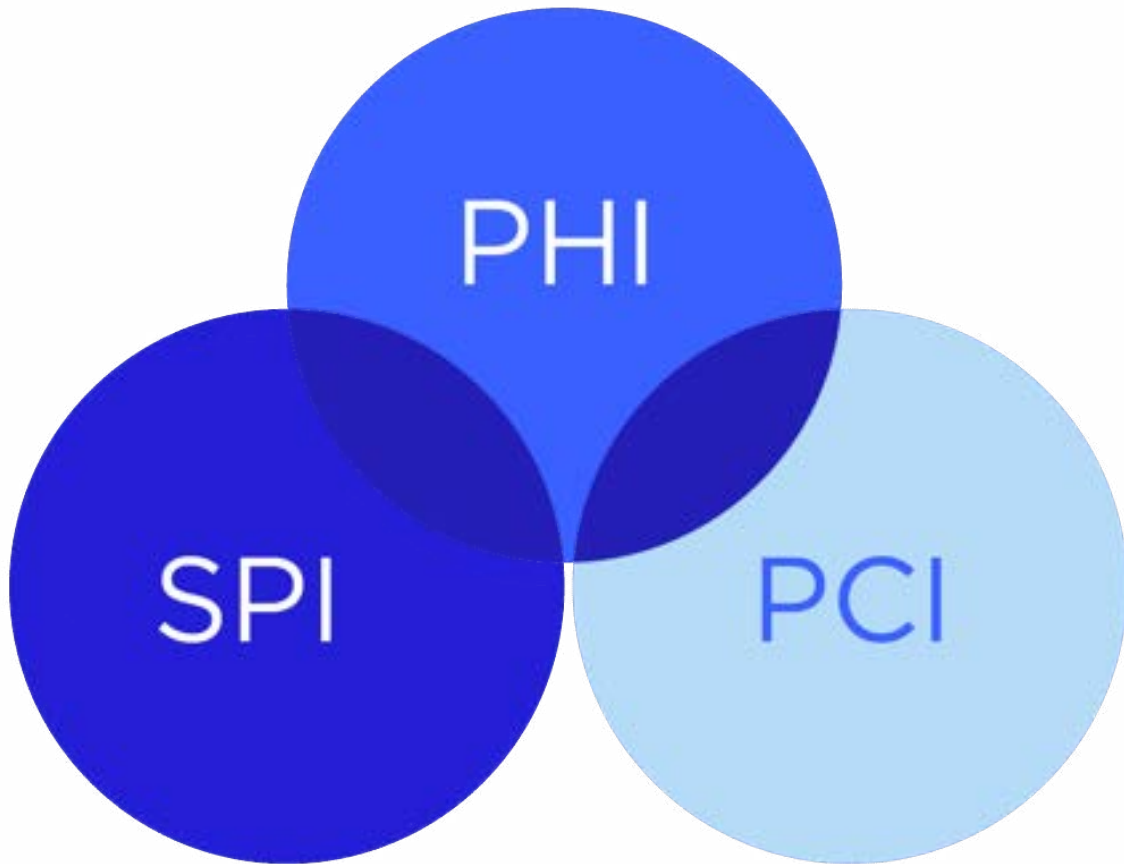
- Cardholder data such as the cardholder's name, the primary account number, the card's expiration date, and security code
- Sensitive authentication data, including magnetic-stripe data, the equivalent data contained on a chip, and the personal identification number (PIN)

Please note that PCI collected in relation to healthcare treatment can also be considered PHI.





# Types of PII



It's important to remember that there is crossover and overlap between the different types of PII.

*Lesson 2 of 9*

# Quiz Break #1

---

Let's take our first quiz break for this training.

---

*Question*

**01/03**

True or False: There is no all-inclusive list of PII.

---

- True, there is no all-inclusive list of PII.
- False, there is an all-inclusive list of PII.

*Question*

02/03

Which of the following data types would be considered PHI when used within a healthcare context? (Select all that apply)

---

Date of Birth

Address

Medical Diagnosis

Eye Color

Education History

Credit Card Information Used for Payment

Blood Test Results

*Question*

**03/03**

True or False: PII can only be one of the following: PHI, SPI, and PCI.

---

True.

False.

# Data Privacy Laws

---



## Data Privacy Laws

Currently, the United States doesn't have just one federal privacy law, but several that cover different types of data or populations. Additionally, several states have passed their own privacy laws to fill in the regulatory gaps with the most prominent state privacy laws coming from California. We'll also cover a major international privacy law from the European Union (EU).

The main privacy laws we'll focus on today are:

- The Health Insurance Portability & Accountability Act of 1996 (HIPAA).
- The Health Information Technology for Economic & Clinical Health (HITECH) Act of 2009.
- The California Consumer Privacy Act (CCPA) & the California Privacy Rights Act (CPRA).
- The European Union's General Data Protection Regulation (GDPR).

This list is not all-inclusive but will provide a good overview of the compliance standards VSP must meet.

## HIPAA & HITECH - Covered Entities & Business Associates

First introduced in 1996, HIPAA outlines the privacy and security requirements for data collected by “covered entities” and “business associates” for purposes of treatment, payment, and healthcare operations. HITECH was passed in 2008 to update these requirements based on the new technology that had become commonplace since HIPAA was introduced.

- **Covered Entities** are healthcare organizations that collect or transmit PHI, such as insurers or healthcare providers.
- **Business Associates** are third-parties that provide a service for or on behalf of a covered entity when the service involves the collection, receipt, storage, or transmission of PHI.



---

Sometimes VSP acts as a covered entity and other times as a business associate to our members. Regardless, we're required to respect their rights and protect their data accordingly.

## HIPAA & HITECH - Member & Patient Rights

Together, HIPAA & HITECH provide our members and patients with certain rights when interacting with VSP and our third-party business associates, such as:

- The right to review the Notice of Privacy Practices which details how VSP uses PHI and privacy rights under HIPAA.
- The right to have PHI use and disclosure limited to purposes of treatment, payment, and healthcare operations unless authorized by the individual.
- The right to ask VSP to limit what PHI we use or share with third parties (unless it relates to payment processing or healthcare services).
- The right to get a list of certain disclosures to third parties of PHI made by VSP.
- The right to access and review the individual's records held by VSP within 30 days of request.
- The right to request updates and corrections to the individual's PHI.
- The right to request VSP use an alternate address when communicating with the individual.
- The right to request restriction of certain uses and disclosures of PHI.

## HIPAA & HITECH - Requirements for VSP

In addition to guaranteeing those rights to our members and patients, VSP and our third-party business associates have the following requirements under HIPAA/HITECH:

- **Limits on Use:** We must only use and disclose PHI in ways set forth in the Notice of Privacy Practices.
- **Limits on Marketing:** We can only use health records for marketing purposes if the individual has expressly agreed to it.
- **Confidentiality:** We must protect PHI as confidential. Any use or disclosure of PHI must be permitted by law or subject to the individual's authorization.
- **Procedures:** We must have written privacy policies and procedures that designate which employees have access to PHI and for what purposes. The procedures must also note how and when PHI can be disclosed.
- **Training:** We must train employees on their privacy procedures and designate a privacy official to assist with enforcement.
- **Enforcement:** We must ensure that appropriate disciplinary action is taken if an employee fails to follow the privacy procedures.
- **Reporting HIPAA Violations:** We must report applicable unauthorized uses and disclosures of PHI to the US Department of Health and Human Services (HHS).

## HIPAA & HITECH - Complaints & Violations

VSP is required to report any violations of HIPAA/HITECH rules to the Department of Health and Human Services (HHS). HHS then leads investigations into alleged complaints and HIPAA/HITECH violations.

The most common complaints, compiled cumulatively, are the following:

- Impermissible uses and disclosures of PHI.
- Lack of safeguards of PHI.
- Lack of patient access to their PHI.
- Lack of administrative safeguards of electronic PHI.
- Exceeding the minimum necessary required PHI for use or disclosure.

# HIPAA & HITECH - Fines & Penalties

In the event of a violation of HIPAA/HITECH rules, both VSP, as an organization, and you, as an individual, can face civil and criminal penalties.

- 1 VSP can face fines up to **\$2M per violation**.
- 2 Individuals found to be knowingly misusing PHI or disclosing it without appropriate controls can be charged as felons with up to **two years in jail and a fine of \$50,000**.
- 3 Additionally, individuals selling or transferring PHI for commercial gain or with malicious intent can face up to **ten years in jail and a fine of \$250,000**.



These penalties are one of the many reasons that it's imperative that workforce members immediately report any potential misuse of PHI to the Privacy Office.

CONTINUE



Let's learn about California's two major privacy laws:

The California Consumer Privacy Act (CCPA) of 2018 and the California Privacy Rights Act (CPRA) of 2020

## The California Consumer Privacy Act of 2018

The CCPA gives California residents more control over how data is collected, processed, shared, or sold by companies.

This law secures privacy rights for California consumers, including:

- The right to know what PII is collected and how it is used and shared.
- The right to delete PII collected (with some exceptions).
- The right to opt-out of the sale of their PII.
- The right to non-discrimination for exercising their CCPA rights.

The CCPA does not generally apply to healthcare information collected for purposes of treatment, payment, or healthcare operations.

## The California Privacy Rights Act of 2020

The CPRA amends and strengthens consumer data privacy rights established initially by the CCPA.

The CPRA established the California Privacy Protection Agency to implement and enforce the law. The CPRA also expands the CCPA privacy rights to include employees, job applicants, and cookie data.

The new law took effect January 1, 2023; enforcement began July 1, 2023.

 Penalties for violations include \$2,500 for each violation or \$7,500 for each intentional violation after notice.

## The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a series of regulations to give residents of the European Union (EU) and European Economic Area (EEA) greater control over their data and information. It establishes stringent rules for businesses to follow when dealing with the data of individuals who interact with them.

It also provides individuals with the following rights:

- The right to be informed of data collection.
- The right of access to their personal data.
- The right to correction of their personal data.
- The right to erasure of non-regulated personal data.
- The right to restrict processing of non-necessary personal data.
- The right to data portability.
- The right to object to processing of personal data.

 Penalties for violations of the GDPR include €10 million or a penalty of 2 percent of the company's worldwide annual revenue, whichever is more.

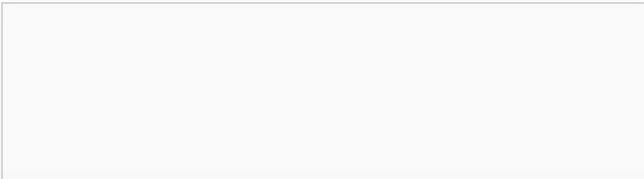
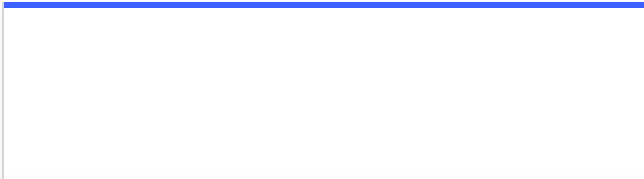


### New & Emerging Privacy Laws

California has led the way for 24 other states to draft and introduce their own legislation on privacy. After California, the first four states to enact privacy laws were Virginia, Utah, Colorado, and Connecticut.

### The Fair Information Principles

Privacy laws continue to be passed by different countries around the world to protect the rights of their citizens and keep up with rapidly developing technology. This may seem daunting from a compliance point-of-view but fortunately for VSP, most laws trace back to the same core concepts known as the Fair Information Principles (FIPs).



## Data Quality

Personal data should be accurate, complete, and up-to-date.

## Purpose Specification

The reason for the collection of personal data should be made clear at the time of collection and not changed without the explicit consent of the data subject.



---

## Use Limitation

Personal data should not be used for purposes other than those specified unless required by law or new consent is captured.

---

## Security Safeguards

Personal data should be protected under reasonable security safeguards.

## Transparency

How and why personal data is being used, stored, or transferred should be made clear in accessible policies.

## Individual Rights

Individuals should have the right to access, correct, obtain a copy of, and (if applicable) delete personal data about them.

## Accountability

The data controller should be accountable for complying with the other principles.

*Lesson 4 of 9*

## Quiz Break #2

---

Let's take another quiz break to see how much you were able to retain.

---

*Question*

**01/03**

True or False: GDPR only applies to EU companies so VSP doesn't have to comply to it.

---

False.

True.

*Question*

02/03

What is the 'minimum necessary' requirement for PHI?

---

- VSP can only collect and disclose the minimum amount of PHI necessary for the task.
- VSP can only market to members or consumers once a week.
- VSP can either text or email members but not both.
- VSP cannot encrypt PHI to make sure it is accessible to members.

*Question*

03/03

Which of the following is NOT a right under HIPAA?

---

- The right to get a list of third parties with whom VSP has shared their PHI.
- The right to request VSP use an alternate address when communicating with the member.
- The right to access and review their records with VSP within 30 days of request.
- The right to delete the PHI VSP has collected on them (with some exceptions).

# Privacy Impact Assessments

---



In order to maintain VSP's compliance to privacy laws and identify risks, the Privacy Office needs to evaluate changes in the way VSP collects, accesses, uses, maintains, processes, and transfers PII.

The Privacy Office evaluates changes through the privacy impact assessment (PIA) process.



To complete a thorough PIA, these questions must be answered:

- What PII is being collected?
- What is the goal of this project?
- How will the PII be protected and maintained?
- Where will the data be transferred?
- With whom will the PII be shared?
- How will this affect the data rights of the people involved?

All projects that change the way VSP collects, uses, maintains, processes, and transfers PII are required to go through the PIA process as a part of the project lifecycle.

- 1 PIAs should be submitted at the beginning of the project before commencement of any testing or piloting.
- 2 This applies to electronic and non-electronic PII.
- 3 PIA completion should be coordinated between the business operations area leader, project manager, and the system/technical owner.
- 4 PIAs can be requested and submitted by emailing: [Privacy@vsp.com](mailto:Privacy@vsp.com)

## Quiz Break #3

---

Let's take another quick quiz break to review when PIAs are required.

---

*Question*

**01/01**

When does a project require a PIA at VSP?

---

- Whenever a project will change the way VSP collects, uses, maintains, processes, and transfers PII.
- Once a year.
- Whenever a project involves third-parties.
- Only when PHI is involved.

# Identifying, Reporting, and Preventing Privacy Incidents

---



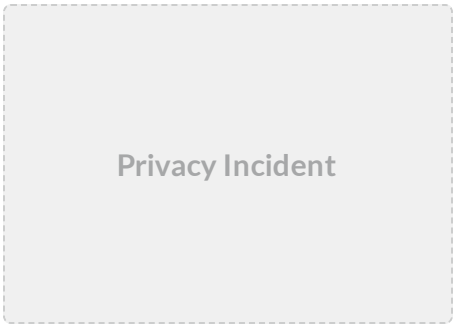
## What is a Privacy Incident?

As a VSP employee or contractor, you are the first line of defense against privacy violations. By properly handling personal data in accordance with well documented and tested processes, you keep us compliant.

A privacy incident report should be submitted any time someone who is not authorized receives, views, or accesses PII.

## Let's Look at Some Examples of Privacy Incidents

Click on the card below and drag it into the correct category to find out which examples are privacy incidents and which are not.



<p><b>Sending personal data to the wrong recipient (mail, email, fax).</b></p>	<p><b>Using personal email to transmit personal data.</b></p>
<p><b>Accessing or disclosing personal data outside of specific business purposes.</b></p>	<p><b>Losing or having your laptop stolen.</b></p>
<p><b>Sharing login details.</b></p>	<p><b>Commingling member/patient information.</b></p>

**Not a Privacy Incident**

**Overhearing your coworker's  
personal phone call at lunch.**

**Getting a spam phone call at  
your personal cell phone.**

**Forgetting your password.**

**Losing your badge.**

---

Click this [link](#) to view the Privacy Incident form.

We recommend bookmarking for future use.

Find quick links to external portals and sites below:

 Concur Expense & Travel	 Contests & Winners (VPN Required)	 Corporate Enterprise Performance Management (Access Required)	 Corporate Services Fast Request
 Corporate Social Responsibility	 Global Safety & Physical Security	 Hearts at Work	 MyADP
 Payroll Dashboard (previously Workcenter)	 Procurement Services Portal	 Product Source	 Purchasing Self-Service (VPN Required)
 Report Privacy or Security Concern	 SAP Reports (VPN Required)	 Service Central	 TimeCard - Amsterdam

You can also find the link to the form on the Quick Links tab on VSP's GlobalView page.

- 1 VSP workforce members are required to report any known or suspected privacy concerns **immediately**. The longer you wait, the bigger the risk for VSP.
- 2 If you are unable to access the form, you can submit via email to [Privacy@vsp.com](mailto:Privacy@vsp.com) or by telephone at 916-858-7432.
- 3 When in doubt, report it.

## Preventing Privacy Incidents at VSP

At VSP, you have the following data privacy responsibilities:

- Identify PII and PHI and know that if data can be used to identify a person or relates to their health, it needs to be protected.
- Protect all PII no matter how or where it is collected or stored.
  - Do not store PII on thumb drives, portable media, or any place it might be lost or stolen.
  - Do not leave PII out on your desk or unlocked when not in use.

- Shred all paper copies of PII when you are done using them.
- Remember that whenever you disclose PHI follow the minimum necessary guidelines.
- Verify the identity and authority of all callers prior to releasing any PII over the telephone.
- Use encryption when emailing personal data outside of VSP.
- Immediately report any unauthorized access or disclosure of PII to VSP Privacy Office.
- Complete a PIA whenever your project will change the way VSP handles PII.



*Lesson 8 of 9*

# Quiz Break #4

---

One last quiz before we finish this training.

---

*Question*

**01/02**

When should you report a privacy incident?

---

- Immediately upon discovery.
- After conducting an investigation.
- Once you've had a chance to involve your manager.
- Within the week.

*Question*

02/02

How can you find more information if you have questions about privacy at VSP?  
(check all that apply)

---

- By emailing [privacy@vsp.com](mailto:privacy@vsp.com).
- By visiting the Privacy Globalview page.
- By calling 916-858-7432.
- By clicking your heels together.

# Training Conclusion

---

## Congratulations!

You completed the VSP Vision New Hire & Annual Privacy Training!

You may now close out of this training to have your progress recorded in the Learning Management System.