vsp vision care

We've Got You Covered

VSP Vision Care Security Overview

VSP Vision Care Security Overview:

vsp vision care

It's Not Just Data—It's People

Successful partnerships start with trust. And above all, you need a partner you can trust with managing sensitive data. VSP® Vision Care is committed to maintaining the security needed to protect the confidentiality, integrity, and availability of your employees' health information. In a heavily regulated industry, we comply with all laws and regulations applicable to our business.

We understand that your selection of VSP as a vision care provider, and your employee's election to enroll in our insurance plan, is largely based on our reputation. We are required by law to protect your employees' data, and we take our responsibility to them very seriously. Unfortunately, we frequently hear about data breaches in the news. So it is crucial that you have confidence in the business partners you entrust with your employees' information.

The VSP policies and procedures are designed to help ensure the safety and security of your employees' health information. Sound security doesn't just happen. It starts with planning, preparedness, execution, and continued oversight. We maintain a comprehensive information security program with detailed safeguards for administrative, technical, and physical security.

> "Keeping your employees' health information secure is about more than protecting data—it's about protecting your employees and their families."

We always strive to earn trust as your business partner, and one of the most important ways we do this is by continuously investing in safeguards for protecting sensitive employee information. Our philosophy is to maintain appropriate and reasonable levels of security—based not just on the requirements of the law, but also the size and complexity of our business, the nature and scope of the services provided to our clients and customers, and the sensitive nature of the employee information we deal with.

VSP approach to information security is to allow access to health information only to those who need it to perform their job. The safeguards we have in place include:

- Unique usernames and complex passwords.
- Encryption of health information shared over public networks.
- Network controls designed to detect and prevent unauthorized access.
- Embedded technical controls to help secure devices like smartphones, laptops, etc. that may access or store health information.
- Regularly-scheduled code review for all VSP software used to deliver vision care services.
- Training on secure development practices for developers.
- Periodic monitoring and testing of VSP systems that process sensitive information to find and address cybersecurity vulnerabilities.
- Policies and procedures that limit physical access to VSP systems.

We require annual security training for all employees, which includes general security awareness training and protocols for accessing, using, storing, transmitting, and disposing of health information.

Keeping your employees' health information secure is about more than protecting data—it's about protecting your employees and their families. We work hard to do exactly that, so you and your employees can enjoy peace of mind.

Secure Data Sharing

VSP shares data with certain third parties in order to provide high-quality products and services to our clients and members.

While VSP does not contract with outside companies to access, process, or store sensitive information for any single client's employees specifically, we sometimes engage third parties to help run our business. These services may include satisfying our contractual obligations, helping keep health information secure, or providing administrative services on our behalf.

For example, VSP allows our network of doctors to access VSP systems to determine eligibility and submit claims, and we allow members to access their benefit and health information online through any web browser. Similarly, VSP leverages the expertise of certain third parties for activities such as partnering to perform disaster recovery services, storing encrypted backup tapes, and processing paper claims.

Some third-party suppliers may have indirect or incidental access to health information. For example, a supplier providing technical support or managed security services may have incidental access to application or system data through screen shots, log files, network traffic, etc.

Evaluating Third-Party Suppliers

VSP accepts full responsibility for third parties who perform services on our behalf. We assess the security practices of all third parties before we engage with them. This multi-step process includes:

INFORMATION SECURITY PROGRAM REVIEW

The VSP Office of Information Security requires each supplier to certify that they have sufficient and appropriate controls in place to meet our security standards. They also must provide contractual assurances, including agreeing to the right of VSP to audit their practices for compliance.

CERTIFICATIONS/INDEPENDENT AUDIT REPORTS

We request that suppliers provide relevant certifications or independent audit reports, including:

- System and Organization Controls (SOC) for Service Organizations Report
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Certifications

BUSINESS ASSOCIATES

Any supplier considered a "Business Associate" under the Health Insurance Portability and Accountability Act (HIPAA) is required to enter into a Business Associate Agreement with VSP, which requires appropriate use of Protected Health Information as prescribed by HIPAA.

Security Audit Process

VSP seeks to continuously evolve and improve its information security program. That's why our information security policies and procedures are periodically reviewed and updated. Likewise, we regularly audit our internal operations to assess our compliance with these policies and procedures.

INDEPENDENT SECURITY ASSESSMENTS

VSP engages independent third parties to perform annual assessments of our information security program to render an official opinion, certification, or attestation of compliance. These currently include the following audits:

- ISO/IEC 27001, Information Security Management Systems Requirements
- SSAE No. 18 SOC 2, Type 2 report
- HITRUST Risk-based r2 Certification

Audit reports are made available to our clients upon request, with appropriate confidentiality terms and conditions in place.

VSP also uses independent third parties to perform periodic vulnerability scans and penetration tests on our public-facing networks and systems. And we perform quarterly in-house vulnerability scans on our internal networks and systems as an additional level of assurance.

Employee Background Checks

Everyone who works at VSP shares the responsibility of keeping sensitive information secure.

That's why all employees, agents, vendors, or other personnel providing services directly to our clients, customers, and members must undergo appropriate background checks and drug screening.

We use leading third-party suppliers to conduct thorough background checks as part of our employee hiring process. The checks include social security, criminal, drug screening, verification of employment, and (when applicable) credit and Department of Motor Vehicle checks. We also check government watch lists like those kept by the OFAC, OIG/GSA, and all state exclusion lists.

Security Incident Management

The statistics on healthcare data breaches are sobering. Between 2009 and 2022, 5,150 healthcare data breaches resulted in the theft, exposure, or loss of more than 382 million healthcare records" That's more than the entire population of the United States.

Keeping your employees' health information safe requires the ability to improve security processes and technology quickly and continuously. That's why VSP focuses on not only protecting data, but also on learning everything we can from attempted attacks on our systems.

We take every actual or suspected security incident seriously, and investigate potential breaches of our systems, including incidences where we discover unauthorized access, collection, use, transmission, disclosure, corruption, or loss of protected health information.

VSP addresses security incidents promptly to reduce client or member impacts and provides relevant information to affected clients, members, and regulatory authorities as required by law.

We comply with all breach notification requirements according to state and federal law, including notifying members if their information has been compromised.

Disaster Recovery

When we see footage of natural disasters on the news, it's easy to focus on the physical damage these emergencies create. However, in the healthcare industry, a disruption in service caused by system failure or data loss can create a secondary crisis that affects millions of people.

As a responsible and trusted business partner, we take disaster recovery seriously and maintain a Business Continuity Plan to ensure prompt continuation of critical business functions. We also maintain a Disaster Recovery Plan to restore our electronic information systems.

We replicate our critical systems and data to a backup facility located in a geographic location that would be unaffected by any disaster impacting our primary data center. This allows us to reasonably ensure our objective of recovering our critical systems within 24 hours, with a maximum of five minutes of data loss.

> "VSP is committed to working with our provider network to allow members to receive timely treatment from their local doctor."

VSP has dedicated employees focused on business continuity and executing our recovery plans. And each division has its own tested business continuity plan to complement our company-wide efforts.

In the event of any significant disaster, VSP is committed to working with our provider network to allow members to receive timely treatment from their doctor.

Summary

VSP appreciates that a lot can happen when employees' health information is shared. Data is a valuable asset, and keeping that vital information secure is paramount. You need to know that the companies you trust with your employees' data can protect it.

You can be confident that VSP has the security policies and procedures in place to reasonably protect the safety and security of your employees' and their families' health information.

We've got you covered.

*(page 5) HIPAA Journal. Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ accessed August 2022.