Security and Privacy at Vim

Vim was designed with privacy and security in mind, utilizing HIPAA, SOC 2, and HITRUST for its framework. Having these solid foundations from the beginning has evolved into a culture that puts customers' privacy and data protection as a top priority.

Culture of Security

SOC 2 Type II + HITRUST

AICPA SOC 2 Type II and HITRUST CSF have become the standard of trust for Fortune 500 companies and the highest security standard for healthcare, respectively. Vim has successfully passed the rigorous external audit of SOC 2 Type II + HITRUST, leveraging the collaboration between AICPA and HITRUST, resulting in the highest level of security and assurance in the healthcare industry.

Dedicated Security Team

Vim's full-time, dedicated security team is led by our Chief Information Security Officer. Comprising seasoned information security professionals, the team has far-reaching control overall aspects of data and product security and is responsible for periodic security and privacy training for all Vim employees. Through close monitoring of market and information security trends and developments, we continuously improve and update our security policies and practices.

Vendor Due Diligence

Supply chain attacks have become a popular method for attackers to gain access to ePHI by targeting insecure third-party services that an organization might use. According to the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS), third-party breaches account for around 25% of ePHI breaches. In response to this risk, Vim has developed a third-party risk management program. New vendors are subject to review by Vim's security team, which performs a security review of the proposed use and the vendor's security posture to ensure that sufficient protections are in place and contractually assured.

Security Operations

Incident Management

Vim incident response procedures are based on industry best practices and are designed to allow swift identification, triage, escalation, notification, and remediation in the event of a security incident. Vim cooperates with its customers in the event that a security incident affects their data and acts in compliance with the HIPAA Breach Notification Rule.

Vulnerability Management

New vulnerabilities are introduced daily and as businesses continue to grow the attack surface grows respectively. Vim has designed and implemented a vulnerability management program aimed at detecting, responding, and mitigating vulnerabilities as soon as possible. By incorporating automated and manual tools and processes to detect both internal and external vulnerabilities, Vim has the ability to detect, alert, prioritize, and respond to emerging threats.

Encryption

Vim encrypts everything, everywhere - as simple as that. By encrypting data at rest and in motion, Vim ensures only those with authorization can actually view the decrypted data. Vim leverages industry recommended encryption protocols and ciphers such as AES-256, SHA-512, and RSA-2048 to protect its customers' data.

Network Security

Vim follows industry best practices and has designed and implemented a highly segregated network with fine-grained access rules, blocking all traffic by default and explicitly allowing access to approved services. Vim's network security architecture also incorporates a Web Application Firewall (WAF) set to protect against DDoS attacks and additional threats.

Application Security

Vim's platform is designed with security in mind, following engineering and deployment best practices as part of Vim's SDLC. Vim continuously evaluates and tests every major feature and the entire platform as a whole to ensure that security and privacy controls operate as intended and provide effective protection. Automated security controls are integrated as part of the continuous integration (CI) process, allowing Vim to detect and remediate issues prior to release. Security testing is performed both internally and externally by security experts who perform penetration testing and security code reviews.

Business Continuity and Resiliency

Backups and Disaster Recovery

Vim has designed and implemented processes, tools, and procedures to ensure minimal disruption to continuous operation, and to allow swift recovery from disaster events.

Privacy

Data Security and Customer Segregation

Vim has implemented numerous access controls to protect and audit access to sensitive data, especially access to Protected Health Information (PHI). Vim utilizes various controls such as User Credentials, Roles, Multi-Factor Authentication (MFA), VPN, and VDI in accordance with the "Need-to-Know" and "Least Privilege" principles. Vim creates distinct environments for each customer, ensuring that there is no commingling of data and that it's only stored and processed in the US.

Encryption

Vim encrypts everything, everywhere - as simple as that. By encrypting data at rest and in motion, Vim ensures only those with authorization can actually view the decrypted data. Vim leverages industry recommended encryption protocols and ciphers such as AES-256, SHA-512, and RSA-2048 to protect its customers' data.

De-identification

Vim is deeply committed to patient privacy and follows the U.S. Department of Health and Human Services (HHS) Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Vim has established processes and procedures to ensure patient anonymity is preserved. No PHI or PII is stored or handled outside of Vim's datacenters.

Questions?

Please reach out to Vim's security team at security@getvim.com.