Veeva SiteVault

HIPAA Checklist for Clinical Research Guide (US Only)

The HIPAA Security Rule establishes standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The general requirements of HIPAA Security Standards state that covered entities must meet:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably-anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably-anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
4. Ensure compliance by its workforce.

How SiteVault Enables HIPAA Compliance

In the course of providing services and system access to customers, Veeva monitors the use of the system and occasionally views customer data as needed to provide system administration and end user support. Veeva administers the system on behalf of customers for Veeva SiteVault (free and enterprise versions). While Veeva has implemented policies and procedures to enable sites to be compliant, local regulations, internal policies, and procedures should always be followed.

Technical Controls

HIPAA Standard	How Veeva SiteVault Supports the Standard	Customer Engagement
Access Control Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.	The first Research Organization Administrator is set up by Veeva for the customer. Additional accounts are created and maintained by the customer's Administrators(s). Veeva employees, including product support, are trained on Veeva's HIPAA Policy.Veeva's policy on this process can be requested as needed.	Complete registration form, including the contact information for the first Administrator, and accept the Terms of Service.
Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.	Each user has a unique account with strong non reversible password security.	Administrators will create user accounts for each study team, monitor, or auditor, and assign system roles and permissions according to internal processes.
Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency.	Veeva personnel are assigned training on policies and procedures based on job function. See HIPAA Policy	Administrator to contact SiteVault support to obtain electronic health information in an emergency and create an internal SOP for such instances.
Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Sessions are managed through a secure cookie which determines the duration of an inactive session before timeout.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	For data at rest, documents are stored using AES 256-bit encryption. Documents are also stored in Amazon Web Services' (AWS) S3 buckets, where an additional AES-256 layer of encryption is applied. Data in transit is encrypted for transmission using TLS1.2 and preferring AES-256 ciphers.	Administrator to ensure proper system roles and permissions assigned to staff and any external users such as monitors, auditors, or inspectors.
Audit Controls Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information	Veeva SiteVault automatically logs all user activity against a record in audit trails that provide visibility into user activity and are a key requirement for compliance with Electronic Records and Electronic Signature (ERES) regulations. Veeva SiteVault users can view audit trail information such as date and time stamp, username, and the event or activity being processed for documents and objects. For example, if a field value is updated, the before and after values are visible in the audit trail for the record.	Users can access the audit trail through the action menu on any document or data field.
Integrity Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Veeva personnel are assigned training on policies and procedures based on job function. See HIPAA Policy and Data Privacy Policy.	Site to follow internal HIPAA and GxP policies and procedures for compliance.

Physical Controls

HIPAA Standard	How Veeva SiteVault Supports the Standard	Customer Responsibility
Facilities' access control — these are policies and procedures for limiting access to the facilities that house information systems. Controls could include contingency operations for restoring lost data, a facility security plan, procedures for controlling and validating access based on a person's role and functions, and maintenance records of repairs and modifications to the facility's security. Workstation use — addresses the appropriate business use of workstations, which can be any electronic computing device as well as electronic media stored in the immediate environment. For example, the workstation that processes patient billing might only be used with no other programs running in the background, such as a browser.	Veeva SiteVault is hosted in the cloud using Amazon Web Services (AWS) resilient hosting platform, providing industry leading resilience for power and internet connectivity whilst maintaining robust physical access control. Please refer to https://aws.amazon.com/compliance/data-center/perimeter-layer/ At no time do Veeva employees use their corporate workstations to view patient or other protected health data.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Workstation security — requires the implementation of physical safeguards for workstations that access ePHI. While the workstation use rule outlines how a workstation containing ePHI can be used, workstation security standard dictates how workstations should be physically protected from unauthorized access, which may include keeping the workstation in a secure room accessible only by authorized individuals.	Veeva workstations are tightly controlled through administrative and technical policy enforcement for the development of Veeva SiteVault.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Device and media controls — requires policies and procedures for the removal of hardware and electronic media containing ePHI in and out of the facility and within the facility. The standard addresses the disposal and the reuse of media, recordkeeping of all media movements, and data backup/storage.	AWS stores and processes each customers' content only in the AWS Region(s) chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required. Please refer to AWS Privacy and Data Protections	Site to follow internal HIPAA and GxP policies and procedures for compliance.

Administrative Controls

HIPAA Standard	How Veeva SiteVault Supports the Standard	Customer Responsibility
Security management process — includes policies and procedures for preventing, detecting, containing, and correcting violations. A critical part of this standard is conducting a risk analysis and implementing a risk management plan.	Veeva SiteVault has a dedicated security team reporting to the Chief Information Security Officer and a Data Protection Officer to ensure our products are compliant with security and privacy requirements worldwide. The Information Security and Data Protection Officers help business managers, users, IT staff, and others fulfill their information security and privacy responsibilities. Plans, policies, and procedures are in place to ensure that there is accountability for the security and use of information assets. See Data Privacy Policy and HIPAA Policy.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Assigned security responsibility — requires a designated security official who is responsible for developing and implementing policies and procedures.	Security personnel receive ongoing training in all aspects of enterprise security from leading vendors and industry experts. The Security team reporting to the CISO consists of 3 teams: Security Operations (SecOps), Security Engineering (SecEng), Security Audit&Compliance. The Chief Information Security Officer assesses external parties for information security compliance based on industry standards such as ISO 27001, Trust Service Criteria, or shared assessments.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Workforce security — refers to policies and procedures governing employee access to ePHI, including authorization, supervision, clearance, and termination.	Veeva SiteVault has an information classification scheme to ensure such information has adequate protection of confidentiality, integrity, and availability.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Information access management — focuses on restricting unnecessary and inappropriate access to ePHI.	The Information Security & Privacy Procedures policy specifies security controls including multi-factor authentication, replication, encryption, and monitoring requirements, by content category.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Security awareness and training — requires the implementation of a security awareness training program for the entire workforce of the covered entity.	All personnel are trained to immediately report security incidents. Such breaches are handled via documented procedural controls and reporting mechanisms. Timely customer notifications are part of this process.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Security incident procedures — includes procedures for identifying the incidents and reporting to the appropriate persons. A security incident is defined as “the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.”	Veeva SiteVault has implemented a backup and recovery strategy with a four-hour recovery point objective (RPO) and a 24-hour recovery time objective (RTO). Disaster Recovery site data is backed up to AWS S3 nightly and stored for 2 years.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Contingency plan — requires plans for data backup, disaster recovery, and emergency mode operations. Evaluation — requires periodic evaluation of the implemented security plans and procedures to ensure continued compliance with HIPAA Security Rule.	Backups are verified using automated daily restore scripts, with fully rehearsed disaster recovery tests performed every month and restore tests at least twice per year.	Site to follow internal HIPAA and GxP policies and procedures for compliance.
Business and associate agreements — requires all covered entities to have written agreements or contracts in place for their vendors, contractors, and other business associates that create, receive, maintain or transmit ePHI on behalf of the HIPAA covered entity.	Veeva has partnered with Amazon to leverage Amazon Web Services for hosted cloud infrastructure. A Master Subscription Agreement is maintained on behalf of this partnership.	Site to follow internal HIPAA and GxP policies and procedures for compliance.