
apervita
Security and Privacy
White Paper
apervita.com

apervita

Introduction

The immense benefits of electronic health data, computing, and collaboration for health enterprises bring with them significant legal and regulatory considerations and challenges. If compliance with HIPAA, HITECH and other frameworks for protected health information (PHI) represents the basic industry standards for health enterprises, Apervita looks beyond them by drawing on security and privacy best-practices from other industries with stringent requirements, such as banking, finance, defense, and communications. In this way, Apervita can address the unique requirements of the health industry while leveraging security and privacy best practices to facilitate making health computable and collaborative. The Apervita platform is underpinned by secure, HIPAA compliant infrastructure, designed for the challenging health data requirements and environment. Apervita's platform architecture was conceived from the ground-up to provide our customers security, availability, and scalability of health analytic & data applications. Apervita secures all data — including PHI — for health enterprises, providing confidence that data is protected, meeting the requirements of the most demanding data privacy and security officers. Our mission is to provide our customers a safe, secure, and private health analytics and data application platform.

01 Security Program

Apervita believes security & privacy are vital to the business operations of its customers. Apervita's security & privacy policies, procedures, platform, and infrastructure are designed to ensure the confidentiality, integrity, and availability of customer information assets. This document will provide details on each of these layers and how they build upon each other to provide a secure environment for our customers.

1. Security Program

1.1 Guiding Principles

Three guiding principles lay at the heart of Apervita's approach to security.

Customer Ownership & Control

Our customers retain ownership and control over all of their data, analytics, applications, and other assets. The impact of this principle can be seen from the customer's complete control over granting & revoking of access and privilege to their users, data and others assets. This includes, but is not limited to, operations such as data and asset load, data retention and purge decisions.

Least Privilege & Minimum Necessary Access

Apervita designs and operates all systems under the concepts of least privilege and minimum necessary access. Customers can grant and revoke specific access to their users and partners to ensure any individual only has the minimum necessary access to perform their designated function. Apervita developers and support personnel only have access to the systems and code necessary for their role. Separation of duties ensure that the developers building code in development environments do not have access to production systems or data. Stringent change control procedures must be followed for updates to the production environment and only a small designated production support team has the access to migrate updates to the production environment. Apervita has ISO 27001:2013 certification and is HIPAA compliant and is routinely audited to reaffirm such status. Apervita also undertakes routine third-party external penetration testing and application black box assessment to the security of our environment. Apervita's platform leverages secure Infrastructure as a Service (IaaS) hosted and supported by US-based hardware, services, and personnel.

Shared Responsibilities

Security is a shared responsibility between Apervita and our customers. By clearly modeling the various layers illustrated below, it becomes easier for all parties to articulate the division of duties and coordinate actions to effectively protect their data, analytics, applications, and other assets.

Customer
Responsibility for
Secure Usage & Access
Provisioning

- Asset Ownership & Governance
- User & Affiliate Entitlement Management
- Organization, Workspace & Asset Management
- Customer Operating System, Network, & Storage

Apervita
Responsibility for
Security of the Platform

- Platform Services
- Platform Archhitecture, Development & Operation
- Operating System, Network, & Firewall Configuration
- Server Side Encryption | Data Encryption | Network Encryption

Cloud Provider
Responsibility for
Security of the Cloud

- Infrastructure Services
- Compute | Storage | Database | Networking
- US-based Infrastructure Hardware
- Regions | Availability Zones | Edge Locations

2. Platform Infrastructure

Apervita hosts its platform and services utilizing Infrastructure as a Service (IaaS) from a leading cloud provider. Their data centers provide a hardened facility with world-class physical security controls. By leveraging IaaS, including its data centers & services, Apervita can provide a HIPAA compliant infrastructure with robust resilience and scalability. Data center controls include, but are not limited to, the controls below:

2.1 Data Centers

Apervita's use of IaaS has been designed to be HIPAA compliant solely using US-based data centers, services, and support personnel. Data center staff have no access onto Apervita systems or access to customer data. While our cloud provider retains sole physical access to the underlying hardware, all data is encrypted and inaccessible to them or their vendors.

2.2 Physical Access

A secured perimeter controls physical approaches to the data center ingress points while interior checkpoints, doors, and locks restrict access within the facility. Apervita's cloud provider follows the least privilege practice when reviewing and approving access to employees, vendors, and visitors. Multi-factor authentication mechanisms are used to access server rooms and log entry. Surveillance & Detection Closed Circuit Television (CCTV) cameras equipped with image recording and storage capabilities monitor key locations. Intrusion detection systems sound alarms if doors are forced open without authentication or held open. 24x7 security officers are on staff and coordinate with local data center personnel to respond to security incidents.

Apervita's cloud provider engages independent third parties to conduct audits and assessments of their security controls. They maintain numerous certifications such as Cloud Security Alliance (CSA), SOC 1 (SSAE 16), SOC 2, and SOC 3 for its Data Centers and Cloud Service Offerings.

2.3 IaaS BAA

Apervita has a Business Associate Agreement (BAA) with our cloud provider and their access to infrastructure is monitored by their policies which earned numerous industry recognized certifications such as Cloud Security Alliance (CSA), SOC 1 (SSAE 16), SOC 2, and SOC 3, ISO 27001, ISO 27017, ISO 27018. Apervita's use of IaaS has been architected and designed to solely use HIPAA eligible services for the processing and storing of PHI.

3. Platform Architecture

The Apervita platform utilizes a multi-tier architecture which breaks out components into separate isolated server grids located on firewall-protected, private networks. This segmentation in conjunction with tight network access controls based on our guiding principle of least privilege minimizes the potential attack surface and provides significant in-depth defense.

3.1 Multi-Tenant & Multi-Affiliate Architecture

Apervita is a multi-tenant and multi-affiliate platform. Apervita logically segregates all customer data through a strong entitlement framework that is controlled by each customer. Each customer using Apervita has one or more 'virtual private environments' for their enterprise. Our customers can granularly control access to their data, analytics, applications, and others assets.

3.2 Multi-tier Web Architecture

Apervita's platform is designed with scalability & resilience as primary design principles. Each of our primary platform tiers (Web Grid, Computing Grid, and Data Grid) is implemented as a cluster. Our components running on these clusters were designed as cloud applications and are loosely coupled to more easily handle disruptions. This provides resilience in the event of a failure of components, servers, or site instances.

Security

Apervita enforces segmentation between systems in different tiers through restrictive firewall rulesets. Only the communication channels required by the solution are allowed between systems. Even systems within the same layer are restricted in their intra-system communication. Fewer and well defined communication paths reduce the potential attack surface and make it easier to monitor for abnormal activity.

Availability

Apervita's platform is designed with scalability and resilience from the ground up as primary design principles. Each of our primary platform tiers (Web Grid, Computing Grid, and Data Grid) is implemented as a cluster. Our components running within these clusters were designed as cloud applications and are loosely coupled to more easily handle disruptions. This provides resilience in the event of a failure of an application, server, or site instance. Leveraging world class data centers and IaaS provide Apervita a highly secure, HIPAA compliant infrastructure coupled with strong redundancy and scalability. Apervita operates in at least three (3) availability zones. An availability zone is defined as an isolated and independent location. The locations are physically separated, located in lower risk flood plains (specific flood zone categorization varies by region), attached to discrete uninterruptible power supply (UPS) and onsite backup generation facilities, as well as fed via different grids from independent utilities to further reduce single points of failure, and redundantly connected to multiple tier-1 transit providers.

Scalability

Combining our robust architecture with cloud scalability and redundancy results in a solution that can elastically scale up or down horizontally across multiple availability zones to dynamically increase or decrease capacity in the event of changes in load demand or loss of any systems or zones.

3.3 Multi-Environment Infrastructure Architecture

Production, Staging, & Performance Environments

Apervita segments its staging, performance, and production platform environments. These environments are distinct and do not allow operation between them. Further segmentation isolates Apervita's non-production environments from its production environment. Our developers do not have access to any of these environments, further securing the content and migration of code and configuration. Code and configuration updates can only be migrated or promoted to each of these environments by a small, select production support team which follows stringent change control procedures. The non-production platform environments never contain any customer data. This restricts all potential PHI data to the production environment and restricts access to such data to only those granted access by the customer and the production support team.

3.4 Data Encryption

Apervita's platform is designed to only work with fully encrypted data. All PHI data is always encrypted at rest and in transit. Virtual server operating systems use encrypted disk for storage of all data at rest. All communication protocols are encrypted from connections between application components and databases to web browser sessions with customer users to secure data upload/download. Unencrypted protocols are disabled or blocked and are not available even for accidental usage.

- Customers are only able to access the Apervita platform using encrypted protocols
  - Web browser sessions can only use HTTPS
  - Web services can only use HTTPS
  - Uploads of data can only occur via SFTP

- Platform components use encryption for all communication between web, compute, & data grids

3.5 Multi-factor Authentication

Apervita authentication is based on a two-factor authentication model. Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically something a user has such as a mobile phone, token, pin, or e-mail, and the other is typically something memorized, such as a security code or password. This is implemented both for Customer access to the Apervita Platform and for administrative work by Apervita employees.

3.6 Web Browser Support

The Apervita platform requires secure encrypted web sessions using SSL over HTTPS and supports most current web browsers including the latest versions of Microsoft Internet Explorer and Edge, Google Chrome, Mozilla Firefox, and Apple Safari on Mac.

4. Platform Management

Apervita manages its infrastructure in a manner that reinforces its security architecture and in accordance with our organizational processes.

4.1	**Separation of Duties & Least Privilege**	Apervita has mature development and support organizations. Employees are assigned roles per our Software Development Life Cycle (see section 5) that break up platform development and production support. This separation of duties reduces the risk that one individual could write new code and promote to production while bypassing change control or supervision. Permissions are assigned to these roles per our guiding principle of least privilege. Only a small, select production support team has the ability to migrate new code or configurations into the production environment. No one else at Apervita has access to the production systems which are the sole repository of customer data.
4.2	**Administrator Authentication**	Apervita maintains multi-factor authentication for access to its platform by its staff.
4.3	**Security Maintenance & Prevention**	Apervita maintains a security maintenance and prevention program to complement its security architecture and data security, which includes: **Vendor Security Patching Program** **Vulnerability Scanning** **Antivirus Protection** **Intrusion Detection & Prevention (IDS)** **Denial of Service (DoS) Protection** **Security Information & Event Management (SIEM)** .
4.4	**Business Continuity**	Apervita includes business continuity planning into its security program for its company and platform operations to provide continuous operations as well as address the HIPAA availability requirements. This involves coordination of platform & application architecture and design with infrastructure redundancy and resilience. Apervita undertakes at least annual business continuity testing for its platform operations and its corporate operations.

5. Platform Development

A software development life cycle (SDLC) provides the methodology for how an organization plans, designs, builds, tests, and deploys software. Apervita's SDLC is based on an agile methodology, coupled with DevOps & ProdOps practices to both speed up deployment while ensuring high quality operations. We build security into our platform development by integrating controls into the procedures for each stage of our SDLC.

5.1 Plan & Design

Apervita believes security must be considered at the very beginning of any development effort. Our requirements gathering, feature prioritization, and design processes consider how our regulated customers will be able to make use of our platform without putting themselves, or their data, at risk. This helps us avoid the common trap of building a solution and then retrofitting security controls into place after the fact. Key Components Include:

Security Architecture

Security Features

External Review

5.2 Build & Test

All Apervita employees take yearly HIPAA and general security training to reinforce the importance of proper handling of Protected Health Information (PHI) data and following corporate security procedures. Just as our plan & design phases incorporated security concerns into the decision process, Apervita developers are mindful of how they develop, test, and validate new code. Key components include:

Peer Code Reviews

Static Code Analysis

Customer Data Isolation

Scale Testing

5.3 Package & Release Separation of Duties

Separation of Duty and Least Privilege are important pillars of our deployment controls. Our developers (and other Apervita staff) do not have access to our production environment nor can they promote platform code or configuration changes into the production platform or any of the primary testing and staging environments. Instead, they must follow our Change Control procedures. Once changes are approved, our small, select production support team handles all scheduled updates.

5.4 Operate & Monitor

Security continues into our operate phase. Apervita conducts third-party black box and white box penetration tests at least yearly, including:

Vulnerability Testing

Application Security Testing

6. Data Security

Apervita has developed a data-centric security model to protect our customers' data, including PHI. Our supporting policies and controls which stretch across our applications, systems, and procedures are based on our guiding principles of customer data ownership and least privilege. These controls are listed below.

6.1	**Ownership**	Apervita customers maintain full ownership of their data on Apervita. Apervita does not have secondary use rights or platform access unless granted by the customer.
6.2	**Access Control**	Customers control all data access and authorization for each of their own Apervita Workspaces via the Workspace Administration. Apervita accounts are entirely administered and controlled by the customer administrator. Workspace Administrators determine access for their accounts, analytics and data.
6.3	**US Data Storage**	All Apervita customer data is stored within the United States.
6.4	**Environment**	All Apervita customer data is only stored in the production platform environment. Customer PHI data is not used for any other purpose. Application and server logs are configured so that they do not include any PHI. No customer data is stored on Apervita workstations or in development environments.
6.5	**Encryption**	All Apervita customer data is encrypted at rest. All data is also encrypted in transit. Web browser access by users and Web Services can only be accomplished using HTTPS. Apervita supports TLS 1.2 and above. All data upload/download processes use secure protocols such as SFTP.
6.6	**Web Service Access**	Web Service requests to Apervita must be digitally signed and include information to authenticate the requestor.
6.7	**Transportation**	Organizations using Apervita transport data to the Apervita platform using secure and encrypted mechanisms such as SFTP and Web Services over HTTPS.
6.8	**Retention & Disposal**	Data retention is controlled by the customer. Data can remain in the account for as long the client maintains an active agreement with Apervita. The customer can choose when to purge and what data should be removed at any time. Apervita logically segregates all customer data through strong entitlements. Data purging is secure and cannot be recovered.
6.9	**Segregation**	Apervita replicates data across at least three availability zones.
6.10	**Replication**	Customers can download data through secure protocols such as HTTPS & SFTP. Data purging is secure and cannot be recovered.

7. Corporate Operations

Apervita's corporate operations provide the security controls across the organization. This includes details of our security team, corporate office systems, staffing, training, and the policies and procedures detailed in our Information Security Management System (ISMS). Together, they build and maintain Apervita's program and develop policies, procedures, and training to support our operations.

7.1 Corporate Infrastructure

Apervita has implemented a policy where its Platform and customer data, independent of type, is kept separate from Apervita corporate data and systems. Our platform is separate and isolated from our corporate systems. It can only be accessed by a small, select production support team. All other Apervita staff are restricted to our corporate systems and do not have access to the Platform systems.

7.2 Security Team Security

The Apervita Security Program is led by its Information Security Officer (ISO) and a team of security professionals. In addition, Apervita retains certain health care security and HIPAA specialists to provide ready access to outside perspectives and expertise.

7.3 Process, Policies & Procedures

Apervita's processes, policies and procedures are designed to ensure the confidentiality, integrity, and availability of its customers' data, analytic, applications, and other assets — in particular, PHI. Apervita implements our guiding principle of least privilege both internally and on its production platform.

Information Security Management System (ISMS)

Apervita has implemented a series of controls and a set of policies & procedures that govern its activities using the ISO/IEC 27001:2013 standard as its Information Security Management System (ISMS). The ISMS combines documented controls and procedures with user training to achieve consistent and repeatable security operations. Apervita works with external third-party vendors for auditing and certifying its implementation and practice of ISO/IEC 27001:2013 standards.

Protected Health Information (PHI) Handling Procedures

Apervita has documented PHI handling procedures that describes management policies on how PHI data is handled at the company.

HIPAA BAAs

Apervita provides and requires Business Associate Agreements (BAA) with all required vendors and partners that perform functions or activities on behalf of, or provides certain services to, Apervita that involve access by the Business Associate to PHI.

7.4	**Incident Response**	Apervita has an incident response plan. All incidents are tracked per Apervita's incident management procedures. Apervita's incident team includes its CISO and CTO, along with specialist legal counsel and forensics teams. Apervita's plan is tested at least annually. Apervita will notify customers of any security incidents in accordance with our terms of service and regulations.
7.5	**Employees and Contractors**	**US Only Employees and Contractors** Apervita's employees and contractors are all based in the United States. Apervita does not employ offshore employees and does not allow contractors or vendors to provide non-US staff access to data, applications or systems.
7.6	**Insurance**	Apervita maintains industry-standard commercial general liability, corporate professional errors & omissions, cyber-liability insurance, workers compensation, and automobile policies.

8. Compliance Assessment & Validation

Apervita believes that independent assessment and validation of security controls is an essential foundation of our security program. Apervita is HIPAA compliant, ISO27001 certified, and is routinely audited to maintain them. Apervita also regularly evaluates its regulatory obligations and adjusts its assessment program based on these requirements.

8.1	**US HIPAA/ HITECH 5010 Compliant**	Apervita is HIPAA compliant and undertakes an annual review to maintain this status and maintains a HIPAA risk assessment. We also retain an outside HIPAA specialist to provide independent expertise and guidance for corporate operations as well as platform development and operations. Apervita's last review was conducted by Semel Consulting in October 2017.
8.2	**ISO/IEC 27001:2013 Certified**	ISO 27001 is an internationally accepted security framework. Apervita is ISO 27001 certified and undertakes an annual review to maintain this status. Apervita ISO 27001:2013 was independently certified by DNV GL Business Assurance in April 2018.
8.3	**SOC1, SOC2, SOC3 Compliant IaaS**	Apervita's cloud operator maintains numerous credentials that include SOC 1, SOC 2, & SOC 3 certifications.
8.4	**FedRAMP**	Apervita does not currently host its platform in a FedRAMP cloud environment or undertake FedRAMP certification. FedRAMP is not a HIPAA requirement. However, should a customer require this additional level of security controls, Apervita can provide its platform in Amazon's AWS FedRAMP compliant GovCloud.
8.5	**Independent Security Testing**	In addition to audits and certifications, Apervita maintains a security testing program using external and independent, third-party vendors. **External Penetration Testing** **Application Blackbox & Whitebox Testing**

9. Customer Responsibilities & Best Practices

Security and compliance are a shared responsibility between Apervita and the customer. This shared model can help relieve customer's operational burden as Apervita operates, manages and controls the platform components from the platform-as-a-service through to the infrastructure with Apervita's infrastructure-as-a-service provider including host operating system down to the physical security of the facilities in which the service operates. In order to ensure a high standards of security and privacy, customers of cloud services should follow industry best practices to keep their data, analytics, applications and others assets safe and secure. While vendors have a responsibility to ensure their platforms and services are built to a high standard of reliability and security, it is also incumbent upon customers to manage and control their use of these platforms. Detailed recommended best practices are available for customers upon request.