Ovation LIMS Security Overview

As diagnostic labs trust Ovation with sensitive patient information, security and reliability are an integral part of what we do. We're committed to protecting customer data with the highest standards. We've put forth a robust set of practices that protect against our workforce or our software compromising customer data availability, integrity, and confidentiality in the Ovation LIMS.

Infrastructure and hosting

The infrastructure supporting our web-based application is leading cloud provider Amazon Web Services (AWS). We chose to host our platform on AWS for the following reasons:

- Security: AWS is designed to meet the most stringent security requirements in the world. Infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of data. The list of AWS certifications, including HIPAA/HITECH, ISO 27001, ISO 27018, and SOC reports 1, 2, and 3, is available here.

- Availability & Performance: AWS delivers the highest network availability of any cloud provider due to their fully redundant 100 GbE fiber network backbone.

Our production infrastructure is implemented within a virtual private cloud (VPC) protected by firewalls, subnets, security boundaries, and IP-whitelisting for intra-system interactions.

Availability

The groups of AWS data centers that host Ovation LIMS are located across multiple isolated and physically separate "availability zones" within a geographic area, which dramatically reduces the risk of outage due to local conditions. Each availability zone has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks.

Our software is stateless and operates across multiple processing nodes so that it can scale up as needed and “fail-over” seamlessly in the case of one node failing.

Our operations staff is available 24/7 to respond in the event that a production incident causes our service to be unavailable or impaired.

Data integrity and backup

Ovation stores customer data in AWS’s RDS (for structured data) and S3 (for documents) services. AWS meets the highest standards for data protection. Customer data are at minimal risk of loss due to nightly RDS backups (executed and stored safely within AWS), redundant S3 storage, and document version retention. Furthermore, data only reside in the U.S.

DATA ENCRYPTION
Customer data transferred, processed, and stored on Ovation are always encrypted using industry best practices. Data are encrypted at rest using AES-256 or better encryption, and in-flight using SSL/TLS 1.2 or 1.3. Cryptographic keys are managed within AWS Key Management Service.

MALWARE DETECTION
We continuously scan the Ovation LIMS infrastructure for viruses and malware.

Security audits

We ensure that Ovation's practices are up-to-date with current standards and insusceptible to the latest vulnerabilities identified by security professionals:

- Ovation LIMS has been independently assessed and SOC 2 Type 1 certified. Ovation demonstrated its internal controls, policies, and procedures are suitably designed and operating effectively to meet the system requirements and service commitments set forth by the Trust Services Criteria and the HIPAA Security Rule (45 CFR Sections 164.308-316).
- Third-party experts perform rigorous annual penetration tests of Ovation
- We use technology that scans our production environment for vulnerabilities and we address those when identified
- New code is automatically analyzed for common security vulnerabilities before it's moved into production
- We subscribe to security vulnerability notices and routinely address them with appropriate patches
- We maintain automatic alerting for actual and potential/emerging issues in multiple layers of our infrastructure

Additional security practices in Ovation LIMS

Ovation LIMS includes several features and measures to promote the safety and privacy of PHI data.

AUTHENTICATION
We partner with a third-party service (Auth0 by Okta) for secure user authentication. Ovation's workforce uses Google single sign-on (SSO) with two-factor authentication (2FA) and strong password policies (including complexity and mandatory changes) to access any system that processes personal health information (PHI). Ovation customers can use two-factor authentication (2FA) or Security Assertion Markup Language (SAML) SSO to access Ovation LIMS. Password policies are also enforced for customers. We have also implemented malicious log-in attempt protection to block suspicious attempts to access Ovation LIMS.

ACCESS CONTROL & ACTIVITY LOGGING
Ovation LIMS supports configurable, role-based access control. All data-modifying operations are audited and users can review these audits within the application.

SESSION MANAGEMENT
Ovation LIMS includes a session management feature that automatically locks out users after 60 minutes of inactivity.

HIPAA compliance

The HIPAA Security Rule establishes requirements to ensure the security and privacy of PHI. Ovation is responsible for protecting the infrastructure that runs all of the services offered in the AWS cloud. Our customers are responsible for ensuring they have a HIPAA compliance program in place and that they use the Ovation LIMS in a manner to ensure their compliance.

Ovation will execute a Business Associate Agreement (BAA) with Ovation LIMS customers. A BAA is a contract between a Covered Entity (the customer) and a Business Associate (Ovation). The contract stipulates how Ovation will handle the customer's PHI and the safeguards we will take to protect it.

OVATION WORKFORCE SECURITY PRACTICES

Our security practices are in compliance with HIPAA and general best practices. Our workforce that may be granted access to systems that process PHI is entirely based in the U.S. and undergoes HIPAA training. We sanction workforce members for policy violations, up to and including termination.

Access to the production environment of Ovation LIMS is limited to operational staff that needs it and is formally approved, tracked, and audited. Access to the underlying infrastructure is further limited and encrypted through a VPN.

Computers used by employees who support Ovation LIMS are password protected and have full-disk encryption turned on. In general, no PHI can be accessed on local/removable devices. It can only be accessed in the cloud.

If workforce members who support Ovation LIMS leave the company, their access to all systems is immediately revoked. All equipment supplied to the workforce member is relinquished.

Our engineering staff members are proficient in secure software development techniques, including the Open Web Application Security Project (OWASP) Top 10, which are confirmed during routine and mandatory code reviews.

THIRD-PARTY VENDORS

Ovation evaluates and periodically reviews the security policies of third parties that Ovation LIMS depends on. Ovation also has a BAA with all third parties that process PHI on our behalf.

We're confident that Ovation will meet your company's security needs, and we invite your questions.

For more information, please contact us at **support@ovation.io**

ovation