OVERVIEW

MedTrainer Security Information

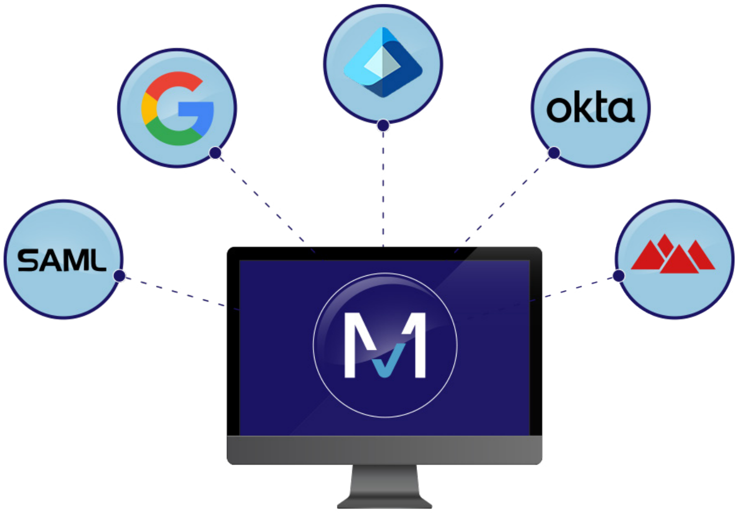
Your organization's data security is mission-critical and we take our commitment to protecting it extremely seriously. MedTrainer's in-house engineering team built the healthcare workforce compliance platform and proactively conducts risk assessments, aggressively tests the security of our products, and continually assesses the infrastructure.

SOC2, SOC3 CERTIFIED

MedTrainer has SOC 2 Type 2 and SOC3 certifications, reflecting our commitment to maintaining rigorous security, availability, processing integrity, confidentiality, and privacy standards. This certification ensures that our systems are designed and implemented with appropriate security controls to protect sensitive data and support our clients' compliance needs.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

Service Organization Control Reports AICPA SOC 3 Formerly SAS 70 Reports



SSO (SINGLE SIGN ON)

MedTrainer uses Auth0, the leading, enterprise-grade authentication and authorization tool as the central authentication layer for all user logins across our products. Plus, users can set up SSO themselves directly in the MedTrainer platform — no need to submit a support request or wait on IT.

Data Security

ENCRYPTION	•**Data in Transit:** Data transferred between the user's browser and MedTrainer's servers is encrypted in transit. MedTrainer uses TLS v1.2. Data transferred between the different infrastructure components of the MedTrainer application are encrypted. This includes communication with external services like email API, and HR integrations. •**Data at Rest:** Data is encrypted at rest: all cloud storage and database tables are encrypted.
CYBER SECURITY INSURANCE	MedTrainer uses commercially reasonable efforts to prevent data breaches and cyber security issues within customer accounts. In the event that there is a breach, MedTrainer maintains the following insurance limits to assist with remedying any fault found as a cause due to MedTrainer's gross negligence: $2M Occurrence / $2M Aggregate.
HIPAA COMPLIANCE	Protected Health Information (PHI) is not stored in MedTrainer's platform, so while MedTrainer has not yet pursued the certification, it maintains HIPAA compliance. MedTrainer's frequent security risk assessments and other precautions are aligned with HIPAA regulations.
INTERNAL POLICIES	MedTrainer maintains a robust set of security policies that are updated periodically to meet the demand of an ever-evolving security environment. Policies are communicated to MedTrainer employees and are available for review at any time.
EMPLOYEE AWARENESS	All MedTrainer employees are required to complete security training. MedTrainer's security team provides continuous education on emerging security threats, and communicates updates with employees regularly. Background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws. New hires sign confidentiality agreements or equivalents upon hire.

WHY HEALTHCARE IT PROS LOVE MEDTRAINER

- Natively-built, cloud-based platform is easy to use and oversee
- Leading HRIS integrations make MedTrainer easy to implement
- Award-winning customer support resolves issues quickly
- Nearly constant innovation with hundreds of in-house product engineers
- MedTrainer's modular approach grows with your organization
- Platform customization is easy — no IT support needed

Data Availability

AVAILABILITY	In the last three years, the application SLA has been greater than 99.95%.
REDUNDANCY	MedTrainer has multiple instances for each production service to support a high load of traffic and to provide redundancy in the case of contingency.
BACKUPS	MedTrainer's production data is backed up daily and tested every quarter. Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.
RETENTION	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.

Application Security

ACCESS CONTROLS	Access to MedTrainer's development systems is limited based on our employee roles and responsibilities. The principle of least privilege is enforced, meaning our employees are given access on a need-to-know basis, specific to their job responsibilities. • Only with a customer request and approval can MedTrainer's support team access customer data. • Non-console access to production is restricted to users with a unique SSH key or access key. • Granular access control allows admins to provide limited-access permissions to certain modules.
QUALITY CONTROL	All changes to our application are subject to peer review, automatic review, manual testing, and automated testing before being available to our users.
MULTIPLE STAGE ENVIRONMENTS	MedTrainer maintains segregated testing, development, and production environments for our development process. Production data is not used in the development and testing environments, unless required for debugging client issues.

DATA CENTER DETAILS

MedTrainer uses Microsoft Azure and AWS as cloud providers for its production servers, databases, and supporting services (firewall, gateways, storage, etc.). These locations are in the U.S. only, mainly in the West.

Vulnerability Management

PENETRATION TESTING	MedTrainer uses third parties to conduct penetration tests to identify deficiencies in the system that may affect critical assets.
VULNERABILITY SCANNING	MedTrainer uses third-party security tools to continuously scan our applications, systems, and infrastructure for security risks and vulnerabilities.
CODE ANALYSIS	MedTrainer's code repositories are regularly scanned for security issues which include the used dependencies and static code analysis.

View MedTrainer's Terms of Service.

MEDTRAINER SECURITY POLICIES AND PROCESSES THAT CAN BE PROVIDED UPON REQUEST

- External Security Testing
- Database Vulnerability
- Software Analysis
- Software Penetration & Network
- Access Control Policy
- Personnel Security Policy
- Password Management Policy
- Cryptographic Control Policy
- Password Management Policy
- Cryptographic Control Policy
- Risk Management and Procedures Policy
- Application Configuration, Change, Maintenance and Release Management Policy
- Configuration Management for Cloud Infrastructure Procedures Policy
- Data Classification, Handling and Retention Policy
- Security Engineering Policy
- Security Hardening Guidelines
- Device Hardening and Patch
- Management Policy
- Cyber Threat Information Management Policy
- Source Code Management Policy
- Supplier Security Policy
- Supplier Security Questionnaire
- Incident Response Plan
- Business Continuity Plan
- Business Impact Analysis
- Third Party Risk Management

Access MedTrainer's Trust Center