Security Overview

Protecting the data behind every patient.

Keena Healthcare Technology was built for the healthcare environment—and that means security is never an afterthought. Every engagement we deliver touches protected health information, mission-critical systems, or both. Our security posture reflects that responsibility, combining enterprise-grade certifications, 24/7 monitoring, and a multi-layered defense strategy designed specifically for healthcare IT.

Security Built for Healthcare. Protected at Every Point.

Security at Keena is not a single control—it is a comprehensive model that spans our infrastructure, our people, and our software. Every point of exposure is addressed, and every layer reinforces the others.

Network & Infrastructure

- Multi-Factor Authentication
- US-based data centers (primary + geo-redundant backup)
- Web Content Filtering
- Email Security (DMARC & Anti-Phishing)
- Data Loss Prevention (DLP)
- Secure Configurations
- Penetration Testing
- Encryption
- Vulnerability Scanning
- Antivirus & Anti-Malware
- Intrusion Prevention Systems (IPS)
- Firewalls

Employees & Access

- US-based workforce
- HIPAA training for all employees
- Role-Based Access Controls
- Least-privilege access principles
- User Access Reviews
- Phishing simulation testing
- Security awareness training
- Web Content Filtering
- Email Security (DMARC & Anti-Phishing)

Applications & Code

- OWASP development best practices
- Static code analysis
- Annual penetration testing on all applications
- Change Management procedures
- Multi-Factor Authentication
- User Access Reviews
- Data Loss Prevention (DLP)
- Secure Configurations
- Secure code-scanning tools
- Encryption & vulnerability scanning
- Azure AD / Microsoft Entra (RBAC)

Our Security Credentials

HIPAA Compliant

All operations, workflows, and data handling processes align with HIPAA requirements for the protection of electronic protected health information.

SOC 2 Type 2

Our core data center operates under SOC 2 Type 2 examination, covering security, availability, processing integrity, privacy, and confidentiality.

HITRUST

For workloads requiring the highest level of healthcare security assurance, we utilize a HITRUST-assessed data center.

24/7 SOC

A fully staffed, around-the-clock Security Operations Center monitors our environment continuously for threats and anomalies.

Annual Testing

We conduct annual stress tests of systems and security controls, including network penetration testing and disaster recovery exercises.

Audit Trails & Access Controls

Every interaction with patient data is logged, traceable, and reviewable. Role-based access controls ensure users see only what they are authorized to see—and every access event is captured in an audit log available for compliance review, internal audit, or regulatory inquiry.

- **Role-Based Access:** Access is granted based on defined roles and least-privilege principles. Administrators control who can access what—and those assignments are reviewed on a regular cycle.
- **Comprehensive Audit Logs:** All user activity is captured in detailed, tamper-evident audit logs. Logs are retained and available for compliance review, internal audit, or regulatory inquiry.
- **Data Retention Management:** Configurable retention and purge policies give organizations control over their data lifecycle—including documented secure destruction when records reach end of retention.

Operational Transparency

We believe transparency is part of security. Clients know when maintenance happens, how changes are managed, and what to expect when something needs attention. No surprises—just a documented, repeatable operational model.

- **Patch Management:** Infrastructure patching runs on a defined bi-monthly schedule. Critical security patches are deployed outside the standard window when the situation requires it.
- **Change Management:** All changes to production environments follow a formal Change Control Board (CCB) process—including planning, testing, authorization, stakeholder communication, implementation, and post-change review. Emergency hotfix procedures are defined separately.
- **Defined SLA Tiers:** Support issues are triaged by severity with committed response times: 4 hours for critical issues, 8 hours for significant impact, and 5 business days for lower-severity items. Planned maintenance windows are communicated in advance.

Security Questions?

We welcome security review conversations and can provide documentation to support your assessment process.

privacy@keenahealth.com | 315.707.7843 | keenahealth.com

Rooted in the United States. Accountable at Every Level.

Every person who touches your data works here—in the United States. Our entire workforce is US-based, our hosting partner is US-based, and we do not use offshore or nearshore support models. This is a deliberate choice. In healthcare IT, accountability is not just a policy—it is a relationship.