RapidAI security and compliance

Providing AI-enhanced imaging with the most secure data management standards

RapidAI sets the standard for secure, compliant deep clinical AI infrastructure. Purpose-built for healthcare, our Edge Cloud platform undergoes a robust set of compliance reviews annually to ensure best in industry compliance to the rigorous security requirements from around the world. RapidAI maintains infrastructure and product security frameworks to ensure a layered approach to threat neutralization including Certifications to ISO 27001 and ISO 27701 standards, with annual conformance assessments to SOC 2 Type 2, CSA STAR, and HIPAA.

In addition, our security team works to ensure adherence to the principles of NIST's Cybersecurity Framework and the new Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile). These frameworks, compliance assessments and certifications combine with other medical device industry standards such as ISO 13485 and ISO 42001 to ensure security concepts and validations are well embedded within our solutions.

As a trusted partner to more than 2,500 hospitals worldwide, RapidAI delivers a secure AI implementation that operates as mission-critical clinical infrastructure, meeting international data protection, security, and AI governance requirements at enterprise scale.

HIPAA COMPLIANT

NIST National Institute of Standards and Technology

ISO 27001 CERTIFIED A-LIGN

ISO 27701 CERTIFIED A-LIGN

A-LIGN ISO 42001 CERTIFIED

TÜV SÜD

STAR CERTIFICATION

NHS

RapidAI.com

Enterprise-grade security architecture

- AES-256 encryption at rest and TLS-secured data transmission to protect protected health information across all environments
- Immutable operating system architecture designed to prevent unauthorized system modification and harden against ransomware
- Containerized microservices deployment to isolate workloads and minimize attack surface
- Continuous infrastructure monitoring and system telemetry to detect operational anomalies in real-time
- Rapid security patching and vulnerability remediation processes to address emerging threats efficiently
- Formal incident response and escalation framework with defined communication protocols
- Secure Software Development Lifecycle (SDLC) including recurring vulnerability assessments and Software Bill of Materials (SBOM) transparency

Secure clinical mobility

- Multi-factor authentication (MFA) to ensure strong identity verification
- Biometric authentication support (e.g., Face ID, fingerprint recognition) for secure, streamlined clinician access
- Configurable session timeouts and device-level safeguards to protect against unauthorized use on shared or unattended devices
- Integration with enterprise Mobile Device Management (MDM) systems to enable centralized mobile policy enforcement
- Secure mobile session handling designed for clinical environments, balancing usability with strict data protection controls

Governance & enterprise oversight

- Centralized user provisioning and permission management aligned with institutional governance policies
- Granular role-based access controls (RBAC) to enforce least-privilege principles across users and roles
- Comprehensive audit logging of user access and system activity to support compliance, accreditation readiness, and internal review
- Enterprise-level utilization analytics and reporting dashboards for oversight of adoption, performance trends, and multi-site consistency
- Configurable data retention policies aligned with regulatory and organizational requirements
- Standards-based integration with PACS, RIS, and EHR systems to preserve data integrity across the enterprise ecosystem