Redox Security Overview

How We Keep Patient Data Safe

Redox is the leading EHR integration platform powering an ecosystem of thousands of healthcare applications. Since exchanging and storing sensitive patient information is at the core of our functionality, keeping data secure is the highest priority at Redox. With that in mind, here's how we keep your data safe through every step of integration.

Securing the Engine

Redox uses industry standard, HIPAA-compliant, and National Institute of Standards and Technology (NIST) recommended encryption standards to protect client information. Redox is hosted in Amazon Web Services (AWS) Eastern Region and wehave a business associate agreement (BAA) in place with Amazon. Our databases are 256 bit AES encrypted.

- The Redox API scales to balance traffic across available application instances. Our endpoints receive automatic security updates, and we force HTTPS at the endpoint layer.
- Application code runs in Docker containers in the app layer. Code changes deploy without interrupting traffic.
- All Redox applications and databases are redundant across AWS Availability zones, so if an outage occurs in one, we failover with minimal interruption to traffic.
- App and database containers run in a private subnet, inaccessible from the outside internet. Access is restricted to the app and bastion layers.
- Database filesystems are encrypted with AWS managed keys. Encrypted backups are taken nightly and stored in a separate geographic location.

HITRUST Certified

Beyond being HIPAA compliant, Redox has pursued and passed an extensive compliance verification from HITRUST, the leading and most widely recognized third-party auditing framework within healthcare. HITRUST evaluates enacted security measures against multiple industry standards and regulations to prove platform compliance. A rigorous and challenging test, our HITRUST certification demonstrates to our partners that data security is a top priority at Redox.

When it comes to selecting third-party vendors, data security is the biggest concern for health systems, who need to know that an outside application will not compromise patient data. Our HITRUST certification allows you to approach health systems with a trusted integration partner who's certified by the highest authority in data security to exchange, process, and store patient data securely.

VPN Security

TCP traffic from Health Systems is encrypted via a secure VPN connection. We use an IPsec protocol to ensure all traffic within the VPN is encrypted and authenticated. The VPN is consistently monitored with a heartbeat to ensure the connection is healthy.

Independent Audits

Redox contracts third party companies to perform independent auditing:

- Veracode performs quarterly Manual Penetration Testing to identify potential system vulnerabilities and confirms our system is properly defended against malicious attacks.
- Veracode also performs quarterly code audits to scan our code base to find and address any security vulnerabilities.
- Intrusion detection is done by Threatstack to monitor all system-level events and report any incongruent activity, like a user promoting their privileges or modifying files.

Operational Security

- All staff are required to apply security protections to their tools, including strong, unique passwords, two-factor authentication to secure systems, endpoint protection, BYOD provisioning controls, and workstation encryption.
- Each employee completes mandatory HIPAA training, general security training, and criminal background checks prior to employment. Additionally, our engineering team completes advanced security training.

Browser Safeguards

- All interactions with the dashboard are handled securely using HTTPS protocols
- Audit logs record all web events, meaning every query or access through the website is always documented. This allows us to know what content is being accessed, when, and by whom.
- We use data concealment as a technique to further prevent inappropriate access to our data. Redox purges PHI content from the dashboard after 48 hours to ensure the narrowest possible window of exposure in the unlikely event that a breach occurs.

Application Connectivity

Between the app and Redox, we use end-to-end encryption to secure all data transmitted over an HTTPS connection. When communicating with health systems, we support and abide by modern industry OAuth standards.

When connecting to third-party applications, we use verification tokens and support OAuth. We store all source API secrets (as well as user passwords) as salted and hashed values for added security.

We're committed to continually working on security enhancements as technology changes and our infrastructure evolves. If you have any questions about our security measures or technology, feel free to reach out to us at **support@redoxengine.com**.