Security Policy

Version: 1.0
Last Updated: June 2026
Contact: naeem@cliniqueue.com

Overview

This document describes CliniQueue's security practices, controls, and vulnerability disclosure policy. It is intended for customers, security researchers, and enterprise procurement teams conducting vendor security reviews.

Reporting a Security Vulnerability

If you discover a security vulnerability in CliniQueue, please report it responsibly.

Contact: naeem@cliniqueue.com
Subject line: `Security Vulnerability Report`
Expected response time: Within 48 hours

Please include:

- A description of the vulnerability
- Steps to reproduce
- Potential impact
- Any proof-of-concept (if applicable)

Do not publicly disclose the vulnerability until we have had a reasonable opportunity to investigate and remediate. We commit to:

- Acknowledging your report within 48 hours
- Keeping you informed of our investigation progress
- Crediting you in any public disclosure if you wish

We do not currently operate a bug bounty program but we deeply appreciate responsible disclosure.

Data Security

Encryption in Transit

All communication with the CliniQueue API is encrypted using TLS 1.2 or higher. HTTP connections are not supported — all requests must use HTTPS. Unencrypted connections are rejected.

Encryption at Rest

All data stored in CliniQueue's Railway PostgreSQL database is encrypted at rest using AES-256 encryption managed by Railway's infrastructure provider (AWS).

Data Minimization

CliniQueue stores the minimum data necessary to provide its service:

- No raw ticket text is ever stored
- PHI is scrubbed before any processing occurs
- Only classification metadata and scrubbed embeddings are retained
- See the HIPAA Compliance Summary for full details of what is and is not stored

---

Authentication & Access Control

API Key Authentication

All API endpoints (except `/health` and `/demo/classify`) require authentication via an `X-API-Key` header. API keys:

- Are generated with cryptographic randomness
- Follow the format `cq_live_[22 random characters]`
- Are scoped to a single customer account

- Cannot be used to access another customer's data
- Can be deactivated immediately by contacting support

Key Security Best Practices

Customers should:

- Store API keys in environment variables, not in source code
- Never commit API keys to version control
- Rotate keys immediately if compromised (contact naeem@cliniqueue.com)
- Use separate keys for development and production environments

Database Isolation

Every database query in CliniQueue includes the customer's API key as a scoping condition. It is architecturally impossible for one customer's query to return another customer's data. This is enforced at the application layer on every read and write operation.

Infrastructure Security

Hosting

CliniQueue runs on Railway, which provides:

- Infrastructure on AWS (us-east-1 region)
- Automatic TLS certificate management
- DDoS protection via Railway's network layer
- Isolated containers per service

Database

- Railway PostgreSQL with encryption at rest
- Database is not publicly exposed — accessible only from the application container
- Connection uses SSL by default

- No direct external database access (no public database port)

Dependency Management

- Dependencies are pinned in `requirements.txt`
- No dependencies with known critical CVEs are used intentionally
- Dependencies are reviewed when updating

Rate Limiting & Abuse Prevention

Monthly Quotas

Every customer has a monthly ticket quota based on their plan. Requests beyond the quota return HTTP 429. This prevents runaway usage from misconfigured integrations.

Request Validation

All incoming requests are validated by Pydantic before processing. Malformed requests return HTTP 422 with details. The `ticket_text` field is required and must be a non-empty string.

API Key Validation

Invalid or inactive API keys return HTTP 401 immediately, before any classification occurs.

Subprocessor Security

OpenAI

- CliniQueue has a HIPAA BAA with OpenAI
- Zero Data Retention is active — ticket text is not logged or stored by OpenAI
- Only Presidio-scrubbed text (PHI removed) is transmitted to OpenAI
- OpenAI maintains SOC 2 Type II compliance
- OpenAI security page: openai.com/security

Railway

- SOC 2 Type II certified
- Railway security page: railway.app/security
- Infrastructure runs on AWS with standard AWS security controls

---

Security Controls Summary

Control	Implementation
Encryption in transit	TLS 1.2+ enforced on all endpoints
Encryption at rest	AES-256 via Railway/AWS
Authentication	API key required on all endpoints
Authorization	Key-scoped database queries
PHI protection	Presidio scrubbing before any processing
Data minimization	No raw ticket text stored anywhere
Audit logging	Every API call logged with timestamp and metadata
HIPAA BAA	Signed with OpenAI and with all customers
Zero retention	Active on OpenAI organization
Dependency security	Pinned dependencies, no known critical CVEs
DDoS protection	Railway network-layer protection

Compliance Certifications

CliniQueue is a small startup and does not currently hold independent compliance certifications (SOC 2, ISO 27001). Customers requiring formal certifications should note:

- CliniQueue's infrastructure providers (Railway/AWS) are SOC 2 Type II certified
- CliniQueue's AI provider (OpenAI) is SOC 2 Type II certified

- CliniQueue operates under a signed HIPAA BAA with all customers and with its AI subprocessor
- CliniQueue follows HIPAA Security Rule requirements for Business Associates as a matter of operational practice

Enterprise customers requiring a formal security questionnaire or third-party audit can contact naeem@cliniqueue.com to discuss options.

Security Incident History

Date	Incident	Impact	Resolution
—	No security incidents to date	—	—

Security Review Cadence

- Dependencies reviewed for CVEs: monthly
- Access controls reviewed: quarterly
- This security policy reviewed and updated: annually or after any security incident