WHITE PAPER

Security & Compliance Technical Specification

Encryption standards, access controls, audit logging, and HIPAA/GDPR technical implementation details for compliance officers and CTOs.

Published:	June 2025
Document ID:	WP-2025-004
Classification:	Public
Author:	ClinixSummary Research Team

1. Executive Summary

Healthcare data is among the most sensitive information in existence. ClinixSummary treats security and compliance not as features to be added, but as foundational architectural principles that inform every design decision. This white paper provides the technical detail that compliance officers, CISOs, and CTOs need to evaluate ClinixSummary's security posture.

2. Encryption Standards

2.1 Data in Transit

All data transmitted between client devices, ClinixSummary services, and external integrations is encrypted using TLS 1.2 or higher (TLS 1.3 preferred). Certificate pinning is enforced on mobile clients. Internal service-to-service communication uses mutual TLS (mTLS) with automatically rotated certificates.

2.2 Data at Rest

All persistent data storage uses AES-256 encryption. Encryption keys are managed through a dedicated Key Management Service (KMS) with hardware security module (HSM) backing. Key rotation occurs on a 90-day cycle with zero-downtime re-encryption.

2.3 Audio Data

Audio recordings are encrypted immediately upon capture and are automatically purged once note generation is complete. Audio is immediately and permanently deleted via cryptographic erasure as soon as the clinical note has been generated. No audio data is ever retained beyond note generation.

3. Access Controls

3.1 Authentication

ClinixSummary supports multiple authentication methods:

- Email/password with mandatory MFA (TOTP or WebAuthn).
- SAML 2.0 SSO for enterprise customers integrating with existing identity providers.
- OAuth 2.0 for API access with scoped permissions and short-lived tokens.

3.2 Role-Based Access Control (RBAC)

A fine-grained RBAC system controls access at the organisation, team, and individual level. Default roles include: Clinician (create/edit own notes), Reviewer (read team notes), Administrator (manage users, view audit logs), and Billing Manager (access billing-related data only). Custom roles can be defined per organisation.

3.3 Data Isolation

Multi-tenant architecture enforces strict data isolation between organisations. Each organisation's data resides in a

logically isolated data partition. Enterprise customers can opt for physically isolated database instances.

4. Audit Logging & Monitoring

Every action within ClinixSummary is logged in a tamper-evident audit trail:

- User authentication events (login, logout, MFA challenges, failed attempts).
- Data access events (note creation, viewing, editing, export, deletion).
- Administrative actions (user management, role changes, configuration updates).
- API calls (endpoint, parameters, response codes, latency).
- System events (deployments, model updates, infrastructure changes).

Audit logs are retained for a minimum of 7 years and are available to organisation administrators through the ClinixSummary Console. Logs are stored in append-only, cryptographically signed storage to prevent tampering.

5. Regulatory Compliance

5.1 HIPAA (United States)

ClinixSummary maintains full HIPAA compliance including: Business Associate Agreements (BAAs) for all US healthcare customers, implementation of all required Administrative, Physical, and Technical Safeguards, regular risk assessments, workforce training, and breach notification procedures.

5.2 GDPR (European Union)

GDPR compliance includes: lawful basis documentation for all processing activities, Data Protection Impact Assessments (DPIAs), data subject rights implementation (access, rectification, erasure, portability), Data Processing Agreements (DPAs), and EU data residency options.

5.3 Additional Frameworks

ClinixSummary also maintains compliance with PIPEDA/PHIPA (Canada), CCPA (California), the Australian Privacy Act, and is pursuing UK medical device registration (MHRA). Our compliance programme is designed to be additive — new regulatory frameworks are incorporated as we expand into new jurisdictions.

6. Incident Response

ClinixSummary maintains a documented incident response plan covering detection, containment, eradication, recovery, and post-incident review. Key elements include:

- 24/7 security monitoring with automated anomaly detection.
- Documented escalation paths and response time SLAs.
- Customer notification within 72 hours for any confirmed data breach (per GDPR) or without unreasonable delay (per HIPAA).
- Post-incident reviews with root cause analysis and preventive measures.

7. Conclusion

Security in healthcare AI is not optional — it is the price of entry. ClinixSummary's security architecture reflects this reality at every layer, from encryption and access controls to audit logging and regulatory compliance. We invite security teams to engage with our detailed technical documentation and to schedule security review sessions with our compliance team.