

HIPAA Compliance Mapping – Current Setup

Purpose: This document maps the current system setup against HIPAA safeguard categories based only on confirmed discoveries. No fixes, recommendations, or implementation changes are proposed.

Status Legend

- = Safeguard is met or partially met based on current evidence.
- = Safeguard is not met based on current evidence.
- = Safeguard status is unknown or not confirmed.

Administrative Safeguards

Safeguard Area	Status	Notes
Written HIPAA policies	■	No documented policies confirmed
Data retention rules	■	Retention periods not documented
Data deletion / disposal	■	Deletion or anonymization process not confirmed
Workforce training	■	No evidence of training processes

Technical Safeguards

Safeguard Area	Status	Notes
User authentication	■	Firebase Auth enforces login
Role-based access control	■	User / doctor / admin roles at app level
Least-privilege enforcement	■	System-wide enforcement not confirmed
Audit logging	■	Partial logs exist; completeness unclear
Encryption in transit	■	Authenticated API communication
Encryption at rest	■	Storage encryption not confirmed

Physical Safeguards

Safeguard Area	Status	Notes
Cloud hosting controls	■	Hosting provider not documented
Physical data center security	■	Assumed via cloud provider, not confirmed
Device & media controls	■	Endpoint protections not documented

Summary: The current system demonstrates some technical safeguards at the application level, while most administrative and physical safeguards remain unknown. Additional clarification is

required before determining HIPAA compliance readiness.