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

Met – Evidence exists that the safeguard is currently in place.

Not Met – Evidence suggests the safeguard is not currently implemented.

Unknown – No confirmation available from code or documentation.

Administrative Safeguards

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

Technical Safeguards

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

Physical Safeguards

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

Summary: The system demonstrates some technical safeguards at the application level. Most administrative and physical safeguards remain unknown and require clarification before

determining HIPAA compliance readiness.