HIPAA Compliance Mapping – Current Setup (Discovery-Based)

Administrative Safeguards

Written HIPAA policies, data retention rules, deletion processes, and workforce training are not confirmed from documentation. Current status for administrative safeguards remains unknown (■).

Technical Safeguards – Access Control

Authentication and role-based access exist at the application level (■). Least-privilege enforcement and separation of identity data from clinical data are not confirmed (■).

Technical Safeguards – Audit Controls

Some audit logging exists for application workflows (■). Completeness of audit logs for image access, authentication events, and retention is not confirmed (■).

Technical Safeguards – Integrity Controls

Clinical workflow integrity is enforced through locked reviews after submission (■). Integrity guarantees for image data are not confirmed (■).

Technical Safeguards – Transmission Security

Internal API communication is secured (■). Encryption in transit to external services or image storage is not confirmed (■).

Technical Safeguards – Encryption at Rest

Encryption at rest for MongoDB, Parse Server image storage, and other external systems is not confirmed (■).

Physical Safeguards

Cloud hosting provider, physical data center controls, and device/media protections are not documented (■).

External Dependencies

Ownership and compliance posture of external systems, including image storage and databases, are not confirmed (■).

Overall Summary

The system demonstrates partial technical safeguards at the application layer. Administrative safeguards, storage controls, retention, and infrastructure protections remain largely unknown. Further clarification is required before determining HIPAA compliance.