SecurePractice – Audit Logging & Retention Policy

Version: 1.0

Applies to: All environments handling ePHI

Effective Date: 12/1/2025

Owner: Security & Compliance Officer

1. Purpose

The purpose of this Audit Logging & Retention Policy is to define how SecurePractice records, monitors, stores, and retains audit logs related to electronic Protected Health Information (ePHI) in compliance with the HIPAA Security Rule. This ensures accountability, traceability, long-term retention, and protection of all audit records.

2. Scope

This policy applies to production systems, Google Cloud Platform services, Firebase products, and all systems processing ePHI.

3. Audit Logging Requirements

3.1 User Activity Logs – login, logout, MFA, password changes, role changes, BAA acceptance.

3.2 Data Access Logs – Firestore/Storage read, write, delete, identity of accessor, IP, timestamps.

3.3 Administrative Activity Logs – IAM changes, network changes, deployments, database config updates.

4. Log Aggregation & Storage

Audit logs are exported to a dedicated HIPAA-compliant bucket:

Bucket Name: hipaa-audit-6yr

Location: global

Retention: 6 years

Restricted access to Security Officers.

Includes admin activity, data access, identity logs, and Cloud Run/Functions logs.

5. Retention Requirements

All audit logs related to PHI are retained for a minimum of six (6) years (2190 days).

Retention is enforced through a locked retention policy preventing deletion or modification.

6. Monitoring & Alerts

Automated detection for unauthorized access, unusual geographic access, failed logins, privilege escalation, and large-volume exports. Alerts routed to Security team.

7. Review & Reporting

Quarterly audit log review and annual compliance audit.

8. Responsibilities

Security Officer – oversight and access control

Engineering Lead – ensure audit generation

DevOps – maintain log sinks and routing

Support Staff – incident response

9. Enforcement

Violations may result in disciplinary action or legal consequences.

10. Revision History

Version 1.0 – Initial policy