ALTNETIX LLC
VitaAI Platform

DATA RETENTION POLICY

HIPAA-Aligned Records Retention Schedule

Control Reference	DATA-16
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

1. Purpose and Legal Basis

This Data Retention Policy establishes retention periods for all categories of records created, received, or maintained by Altnetix LLC. Retention periods are established to comply with HIPAA (45 CFR §164.530(j)), applicable state medical records laws, financial regulations, and legal hold obligations.

2. Retention Schedule

Record Category	Retention Period	Legal Basis	Storage Location
PHI – Patient Records (per BAA)	6 years min (state law may extend)	HIPAA §164.530(j)	Azure SQL + Blob (encrypted)
PHI – Audit Logs	6 years	HIPAA §164.312(b)	Azure Blob (WORM)
HIPAA Security Policies	6 years from last effective date	HIPAA §164.316(b)	Document management
Business Associate Agreements	Term + 6 years	HIPAA §164.504(e)	Legal records
Employee HIPAA Training Records	6 years	HIPAA §164.530(b)	HR system
System Access Logs	1 year operational / 6 years compliance	HIPAA + SOC 2	Azure Monitor
Financial Records	7 years	IRS / state tax law	Accounting system
Contracts and MSAs	Term + 7 years	Commercial law	Document management
Incident Response Records	6 years	HIPAA §164.308(a)(6)	Compliance files
Backup Data	Per recovery objectives (90 days)	Operational	Azure Backup (geo-redundant)

3. PHI Retention Specifics

PHI is retained for a minimum of 6 years from the date of creation or the date when the PHI was last in effect. When a Covered Entity terminates its subscription, PHI is returned or destroyed within 90 days per the applicable BAA. State-specific requirements (e.g., 10 years in some states for certain record types) take precedence over the 6-year federal minimum.

4. Retention Enforcement

Automated retention controls are implemented in the VitaAI platform

where technically feasible. The DbCleanupService runs every 2 hours to enforce operational data retention limits. WORM-protected Azure Blob containers prevent deletion of immutable audit records during the retention period.

5. Legal Holds

When litigation, regulatory investigation, or audit is reasonably anticipated, normal disposition schedules are suspended. Legal holds are issued by the Security Officer in writing. All workforce members notified of a legal hold must preserve relevant records regardless of scheduled disposition dates.

6. Roles and Responsibilities

- Security Officer — maintains this Policy, manages legal holds, approves exceptions
- Engineering — implements technical controls for automated retention enforcement
- HR — maintains employee training and personnel records per schedule
- Finance — maintains financial records per applicable tax and accounting requirements