ALTNETIX LLC
VitaAI Platform

PRIVACY POLICY

Data Privacy, PHI Handling & Patient Rights

Control Reference	CUST-19
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. Introduction and Scope

Altnetix LLC ("Company," "we," "our") operates the VitaAI electronic health record and clinical AI platform ("Platform"). This Privacy Policy explains how we collect, use, disclose, and protect personal information and Protected Health Information (PHI) in connection with the Platform and all associated services.

This Policy applies to healthcare providers, administrative staff, patients, and authorized third-party integrators. It supplements — and does not replace — any Business Associate Agreement (BAA) executed between the Company and a Covered Entity under HIPAA.

2. Information We Collect

2.1 Protected Health Information (PHI)

The Platform processes PHI as defined under 45 CFR §160.103, including patient demographics, medical histories, diagnoses, treatment records, prescription data, lab results, and insurance information. PHI is processed only under written authorization or as permitted by the HIPAA Privacy Rule.

2.2 Account and Operational Data

We collect account registration data (name, email, professional credentials, NPI number), authentication records, audit logs, system usage metrics, and support correspondence. This data is used solely to operate, improve, and secure the Platform.

2.3 Technical Data

We automatically collect IP addresses, browser type, operating system, session identifiers, and referring URLs for security monitoring, fraud prevention, and service optimization. This data is retained for 90 days in operational logs and for 6 years in HIPAA audit logs.

3. How We Use Information

- Providing, maintaining, and improving the Platform and its clinical features
- Processing healthcare transactions and supporting clinical workflows
- Complying with HIPAA, HITECH, and applicable state health information laws
- Detecting, investigating, and preventing security incidents and unauthorized access
- Communicating service updates, maintenance windows, and security notices
- Supporting customer success, training, and technical assistance
- Fulfilling legal obligations, court orders, or regulatory requirements

4. PHI Disclosure and Sharing

We disclose PHI only as permitted or required by the HIPAA Privacy Rule (45 CFR Part 164, Subpart E). Specifically, we may disclose PHI:

- To Covered Entities under an executed BAA for treatment, payment, and healthcare operations
- To Business Associates with appropriate BAAs in place (e.g., cloud infrastructure, analytics)
- As required by law — court orders, subpoenas, law enforcement requests under 45 CFR §164.512
- For public health activities as authorized under 45 CFR §164.512(b)
- In the event of a de-identified disclosure under 45 CFR §164.514 expert determination or safe harbor methods

We do NOT sell PHI or personal information. We do not use PHI for marketing purposes without explicit patient authorization.

5. Security Safeguards

The Company implements the administrative, physical, and technical safeguards required by the HIPAA Security Rule (45 CFR Part 164, Subpart C), including:

- AES-256-GCM encryption of PHI at rest; TLS 1.2+ encryption in transit
- Field-level encryption of sensitive identifiers (SSN, DOB, MRN)
- Role-based access control (RBAC) with least-privilege enforcement
- Multi-factor authentication (MFA) required for all system access
- Tamper-evident audit logs retained for a minimum of 6 years
- Annual HIPAA risk assessments and penetration testing
- Automated threat detection via Microsoft Sentinel

6. Patient Rights

Patients whose PHI is processed by the Platform retain all rights under the HIPAA Privacy Rule, including the right to access, amend, request accounting of disclosures, and request restrictions on use of their PHI. Requests must be directed to the applicable Covered Entity (healthcare provider). The Company will support Covered Entities in fulfilling these requests within required timeframes.

7. Data Retention

PHI is retained for a minimum of 6 years from the date of creation or last effective date, consistent with 45 CFR §164.530(j) and applicable state medical records laws. Upon contract termination, PHI is returned to the Covered Entity or securely destroyed within 90 days per the applicable BAA.

8. Contact and Updates

For privacy inquiries, data subject requests, or to report a potential privacy issue, contact: compliance@altnetix.com. This Policy is reviewed annually and updated as required. The current version is always available at https://vitaai.altnetix.com/privacy.