ALTNETIX LLC
VitaAI Platform

ACCEPTABLE USE POLICY

Information Systems and PHI Handling Standards

Control Reference	IT-11
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 Scope

This Acceptable Use Policy ("Policy") establishes the rules for authorized use of all Altnetix LLC information systems, computing devices, networks, cloud services, and Protected Health Information ("PHI"). This Policy applies to all workforce members including employees, contractors, consultants, and temporary staff ("Users").

2. Authorized Use of Information Systems

Company systems and PHI may be used only for legitimate business and healthcare operations purposes. Users are permitted to:

- Access clinical and operational data necessary for their assigned job responsibilities
- Use Company-issued or approved devices for work tasks during business operations
- Access the internet and third-party services for work-related purposes
- Communicate via Company-approved secure messaging and email platforms

3. PHI Handling Requirements

All workforce members with access to PHI must comply with the following requirements (HIPAA §164.530):

- Access only the minimum necessary PHI required to perform assigned duties
- Never share PHI via personal email, SMS, or non-encrypted channels
- Lock workstations before leaving them unattended (automatic lock after 10 minutes)
- Report any suspected PHI exposure or unauthorized access within 2 hours
- Never download PHI to personal devices or unauthorized cloud storage
- Use only Company-approved de-identification methods before sharing data externally

4. Password and Authentication Requirements

- Minimum 12-character passwords with upper/lower case, numbers, and special characters
- Unique passwords for each system; password reuse across Company systems is prohibited
- Multi-factor authentication (MFA) is required for all systems containing PHI
- Passwords must never be shared, written down, or stored in plaintext
- Password changes required every 90 days and immediately upon suspected compromise

5. Device and Network Security

- Company-issued devices must have approved endpoint protection software installed and active
- Full-disk encryption is required on all devices used to access PHI
- Only approved VPN must be used when accessing Company systems on public Wi-Fi
- Personal devices may access Company systems only through the approved MDM portal
- USB storage devices are prohibited on systems containing PHI without prior approval

6. Prohibited Activities

The following activities are strictly prohibited and may result in immediate termination:

- Accessing PHI or clinical systems without authorization or for personal purposes
- Attempting to circumvent security controls, audit logging, or access restrictions
- Installing unauthorized software on Company systems
- Sharing login credentials or creating shared accounts
- Using Company systems for illegal activities, harassment, or personal financial gain

- Disclosing confidential information or PHI to unauthorized parties
- Connecting unapproved external storage or hardware to Company systems

7. Monitoring and Enforcement

Users are advised that Company systems are monitored for security purposes. Use of Company systems constitutes consent to monitoring. Violations of this Policy will be addressed through the Company's disciplinary process, up to and including termination and referral to law enforcement.