NB-70-25

Device Security and HIPAA IT Controls Policy

Policy Owner	Chief Information Security Officer (CISO)
Effective Date	September 10, 2025
Next Review Date	September 2026
Classification	Internal Use Only

1. Purpose

This policy defines the administrative, physical, and technical safeguards required to protect systems containing electronic Protected Health Information (ePHI). It establishes encryption standards, access controls, monitoring, and breach response requirements in alignment with the HIPAA Security Rule.

2. Scope

Applies to all company-owned laptops, desktops, servers, and mobile devices that store, transmit, or access ePHI; all contractors, employees, and business associates handling ePHI; and cloud-hosted or vendor-managed systems connected to Northbridge infrastructure.

3. IT Security Control Requirements

3.1 Access Controls
- All users must have unique user IDs; shared accounts are prohibited.
- Multi-Factor Authentication (MFA) is required for remote access and administrative accounts.
- Automatic session timeouts after 15 minutes of inactivity.
- Privileged accounts must use separate credentials from standard accounts.

3.2 Audit & Monitoring
- All access to ePHI must be logged (logins, file access, modifications, deletions).
- Logs must be retained for 6 years.
- Daily automated monitoring of critical system logs; monthly manual review by IT Security.
- Alerts must be generated for repeated failed login attempts or unusual access patterns.

3.3 Integrity & Patch Management
- Endpoint protection must be installed on all devices.
- Security patches must be applied within 30 days of release (critical patches within 7 days).
- File integrity monitoring must be used on systems containing ePHI.

3.4 Encryption
- At Rest: All devices containing or capable of accessing ePHI must use full-disk encryption (BitLocker, FileVault, or equivalent).
- In Transit: ePHI must be encrypted using TLS 1.2+ or VPN.
- Encryption keys must be centrally managed and escrowed with IT Security.

3.5 Physical Safeguards
- Portable devices must not be left unattended in unsecured locations.
- Servers storing ePHI must reside in secure, access-controlled facilities.
- Disposal or repurposing of devices must include secure data wipe or destruction.

3.6 Backup & Recovery
- ePHI systems must be backed up daily.
- Quarterly restore tests must validate recovery point objectives (RPOs) and recovery time objectives (RTOs).
- Backup copies must be encrypted and stored in a secure offsite or cloud environment.

3.7 Incident Response
- All suspected or actual compromises of devices containing ePHI must be reported immediately to IT Security.
- Incident Response Team will assess whether the event constitutes a breach under HIPAA.
- Forensic preservation steps must be followed to maintain chain of custody.

4. Breach Risk Determination

- Encrypted Device Compromise: Device is lost or stolen, but encryption was active and properly implemented → Not considered a reportable breach under HIPAA.
- Unencrypted Device Compromise: Presumed breach requiring notification under HIPAA.
- System Compromise (e.g., malware, unauthorized access): Breach determination will depend on whether ePHI was accessed, altered, or exfiltrated.
- Reporting Obligations:
- Breaches affecting 500+ individuals: Notify affected individuals, HHS, and media within 60 days.
- Breaches affecting <500 individuals: Notify affected individuals within 60 days and log/report annually to HHS.

5. Responsibilities

- CISO: Maintains policy, oversees risk analysis, and reports to the Board.
- IT Security: Implements controls, monitors compliance, manages encryption keys, and investigates incidents.
- Department Managers: Ensure employees comply with IT security policies and cooperate in remediation.
- Employees: May not disable, bypass, or ignore security safeguards. Must report lost or stolen devices immediately.

6. Enforcement

Non-compliance with this policy may result in removal of devices from the network until compliance is achieved, escalation to management, disciplinary action for employees, or contract termination for non-compliant vendors.