Hardware, Media Management, and Data Destruction Policy

Note: Sections labeled [HIPAA] apply when systems/media create, receive, maintain, or transmit ePHI. Otherwise, follow the baseline requirements.

1.0 Purpose

Define secure lifecycle requirements for hardware and removable media and the standards for data sanitization/destruction at transfer, reuse, or end-of-life. [HIPAA] Ensure alignment with HIPAA Security Rule.

2.0 Scope

All company-owned/managed endpoints, servers, network devices with storage, and removable media (USB, external disks, tapes, optical, mobile) across all sites and cloud environments. [HIPAA] Applies to ePHI-capable systems/media.

3.0 Roles and Responsibilities

- **IT Asset Management**: Inventory, custody tracking, disposition coordination.
- **IT Operations**: Deployment, maintenance, incident handling; execute sanitization/destruction.
- **Security**: Policy oversight, audits, exceptions; [HIPAA] Security/Privacy Officer approvals.
- **Employees**: Proper custody and use of assigned devices and media.

4.0 Policy Statements

4.1 Asset Inventory and Ownership
- Maintain CMDB inventory with unique IDs, owner, location, configuration, and data classification.
- Track chain of custody for device/media transfers.
[HIPAA] Retain records relevant to ePHI for ≥ 6 years.

4.2 Procurement and Standard Builds
- Use approved hardware standards and secure images/baselines.
- Enforce full-disk encryption (FDE) on supported devices; enable secure boot and TPM.
[HIPAA] Encrypt ePHI at rest/in transit; implement access controls and audit logging.

4.3 Storage and Physical Security
- Store spares/returned devices in locked cabinets with access logs; use tamper-evident seals for data-bearing items.
[HIPAA] Limit physical access to authorized personnel; maintain access records.

4.4 Removable Media Controls
- Restrict media use to business need; disable by default where feasible.
- Encrypt removable media; label with owner/asset ID; prohibit personal media for business data.
- Scan media for malware prior to use.
[HIPAA] Apply minimum necessary standard for ePHI; document approved use cases.

4.5 Transport and Shipping
- Use tracked carriers; tamper-evident packaging; document chain of custody for transfers.
- For high sensitivity, use two-person control.
[HIPAA] Protect ePHI during transport; ensure BAAs with handlers where applicable.

4.6 Maintenance and Repair
- Sanitize/remove drives before third-party service when feasible; otherwise ensure vendor data protection.
[HIPAA] Execute BAAs with vendors potentially handling ePHI; log custody.

4.7 Incident Handling
- For loss/theft, quarantine via MDM/EDR; initiate remote wipe if appropriate; notify Security; document.
[HIPAA] Assess for reportable breach; follow Breach Notification procedures.

4.8 Return, Decommission, and Disposition
- Collect devices on offboarding/replacement; reconcile inventory; proceed to sanitization/destruction per Section 4.10.

4.9 Training and Awareness
- Provide onboarding and annual refresher training on hardware/media handling.
[HIPAA] Include HIPAA device/media handling modules.

4.10 Data Sanitization and Destruction
- Follow NIST SP 800-88 Rev.1: select Clear, Purge, or Destroy based on media type and reuse.
- Document method, tool/procedure, operator, witness, serials, timestamps.
- Verify results (hash/visual/certificate) and file Certificates of Destruction when applicable.
[HIPAA] Maintain documentation for ≥ 6 years; ensure alignment with 45 CFR §164.310(d) and §164.312(e).

4.11 Third-Party Vendors
- Use vetted vendors; obtain certificates for destruction; ensure contractual safeguards.
[HIPAA] Execute BAAs with vendors that may handle ePHI; require adherence to NIST 800-88.

4.12 Compliance and Audit
- Perform periodic audits of inventory accuracy, custody logs, storage controls, and destruction

records; remediate gaps.

5.0 Exceptions

Exceptions require documented justification, risk assessment, compensating controls, and Security (and [HIPAA] Security/Privacy Officer) approval.

6.0 Review

Review annually or upon significant operational/regulatory changes.

Revision #4
Created 16 September 2025 21:57:45 by Travis Woolery
Updated 16 September 2025 22:10:09 by Travis Woolery