

# DATA DISPOSAL POLICY

Secure Destruction of PHI and Company Data

<b>Control Reference</b>	DATA-17
<b>Document Version</b>	1.0
<b>Effective Date</b>	June 1, 2026
<b>Next Review</b>	June 1, 2027
<b>Classification</b>	Confidential – Internal & Customer Use
<b>Maintained by</b>	Altnetix LLC Security & Compliance Team
<b>Contact</b>	compliance@altnetix.com



## 1. Purpose and Scope

---

This Policy establishes requirements for the secure disposal of all data and media containing PHI or Confidential Information. It applies to electronic storage media, physical documents, cloud-stored data, and end-of-life systems. Secure disposal is required by HIPAA §164.310(d)(2)(i) and is a critical control for preventing unauthorized PHI disclosure.

## 2. Electronic Media Disposal

---

### Hard Drives and SSDs

Storage devices containing PHI must be sanitized using NIST SP 800-88 "Clear" or "Purge" methods prior to reuse or disposal. For SSDs and flash storage, cryptographic erasure is the approved method. Devices designated for destruction must be physically shredded by a certified media destruction vendor.

### Cloud Data Deletion

When PHI is deleted from the VitaAI platform per a customer request or BAA termination, deletion is performed at the application and database layers followed by Azure Blob soft-delete expiration. Azure guarantees physical media destruction for decommissioned storage through its NIST 800-88-aligned processes.

## 3. Physical Document Destruction

---

Paper documents containing PHI must be shredded using a cross-cut or micro-cut shredder (NIST P-4 or higher). Documents awaiting shredding must be stored in locked shred bins. Bulk document shredding may be performed by a NAID-AAA-certified vendor with a certificate of destruction issued for each job.

## 4. End-of-Subscription PHI Return/Destruction

---

Upon termination of a customer subscription, the Company will:

- Notify the customer within 10 business days of termination effective date
- Provide a secure export of all PHI in FHIR R4 or HL7 format within 30 days
- Destroy all remaining PHI within 90 days of termination per the BAA
- Issue a Certificate of Destruction confirming PHI disposition

## 5. Certificate of Destruction

---

A Certificate of Destruction is issued for all PHI disposal events, documenting: disposal method, date, personnel responsible, and confirmation that data is unrecoverable. Certificates are retained for 6 years.

## 6. Vendor Requirements

---

All third-party vendors involved in data disposal (shredding, e-waste, cloud decommissioning) must: (a) execute a BAA if they may encounter PHI; (b) demonstrate NAID AAA certification or equivalent for physical media; (c) provide certificates of destruction for all PHI-containing materials.