

The HIPAA Asset Inventory One-Pager

Where the inventory ends: disposal you can prove

promo.ccr cyber.com/articles/hipaa-security-rule-asset-inventory-itad

The HIPAA Security Rule overhaul now targets July 2027. Its asset-inventory requirement is worth starting now, because the inventory is where the rule's existing disposal requirements begin and end.

PROPOSED VS. ALREADY REQUIRED

What would change, and what is required today

Topic	Current rule (in effect)	Proposed rule (not final)
Asset inventory	Implied by the required risk analysis	Technology asset inventory + network map of ePHI movement, reviewed at least every 12 months and on change
Disposal	Required: final disposition of ePHI and the hardware or media holding it — 164.310(d)(2)(i)	Retained; standard renamed “technology asset controls”
Media re-use	Required: remove ePHI before media is re-used — 164.310(d)(2)(ii)	Retained
Accountability	Addressable: record of hardware and media movements and who is responsible — 164.310(d)(2)(iii)	Generally required: the addressable category is removed, with limited exceptions
Business associates	Business associate agreement required	Annual written verification of technical safeguards, with a subject-matter expert analysis

THE END-OF-LIFE LOOP

Lifecycle states that keep a device on the record

- **In service** — assigned, located, holding or transmitting ePHI as mapped.
- **Retired, awaiting disposition** — out of service but still data-bearing, with a storage location and a responsible person. This is the accountability record in practice.
- **In vendor custody** — picked up under a serialized manifest and chain of custody.
- **Disposed** — sanitized or destroyed, with the NIST SP 800-88 method, date, and a certificate tied to the serial number attached to the record.

THE BLIND SPOTS

Devices most often missing from healthcare inventories

Multifunction printers and copiers with internal storage · imaging workstations and modality consoles · laboratory and bedside devices with local storage · workstations on wheels and bedside tablets · network and storage equipment · and the storeroom of retired equipment awaiting a decision. **Quick test:** take last month's certificates of destruction and confirm every serial appears in the inventory and ends there; then check every device marked retired against a certificate. Mismatches in either direction are the gaps.

STARTING NOW

Five steps that hold up under the current or proposed rule

1. Extend the inventory past decommissioning: retired, in-custody, and disposed states, with a location and responsible person. **2.** Map where ePHI comes to rest, not only where it flows. **3.** Require a per-serial disposition record for every data-bearing device, reconciled to the inventory. **4.** Review the BAA with your disposition vendor and the evidence behind it. **5.** Review the inventory at least annually and on every change: new systems, mergers, refreshes, moves.

ASK YOUR ITAD VENDOR

Five questions for your disposition vendor

- Is a business associate agreement in place for every pickup and processing location?
- Does every data-bearing device come back with a per-serial certificate naming the NIST SP 800-88 method and date?
- Can your records be reconciled to our inventory by serial number, including failed and unreadable drives?
- Can we verify your NAID AAA and R2v3 certifications in the issuers' directories, by facility?
- If the proposal is finalized, what would your annual verification of technical safeguards contain?

Sources: HHS, HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, notice of proposed rulemaking (Federal Register, Jan. 6, 2025) and HHS fact sheet; 45 CFR 164.310(d); reporting on the July 2027 final-action target. The proposed rule is not in effect and may change; summaries are not regulatory text. Informational only — not legal advice.