# THE HIPAA POLICY-TO-CONTROL CROSSWALK

## The 14 documents every covered entity and business associate must be able to hand OCR — and the exact regulation each one satisfies.

Based on the HIPAA Security Rule, 45 CFR Part 164 Subpart C, as amended by the HIPAA Omnibus Final Rule (78 FR 5566, Jan. 25, 2013). **This is the rule OCR enforces today.** The Security Rule NPRM published at 90 FR 800 (Jan. 6, 2025) — mandatory MFA, mandatory encryption, elimination of "addressable" — remains **proposed and is not enforced.** Anyone telling you otherwise is selling you something.

| # | POLICY DOCUMENT | SATISFIES (45 CFR) | EVIDENCE OCR ASKS FOR |
|---|---|---|---|
| 00 | **Information Security Program (ISP)** | §164.306(b), (d)(3), (e); §164.308(a)(2), (a)(8); §164.316 | Named Security Official. Annual program evaluation. Addressable determination methodology. 6-year retention schedule. |
| 01 | **Risk Management Policy** | §164.306(a); §164.308(a)(1)(i), (ii)(A), (ii)(B) | Enterprise-wide Security Risk Analysis. ePHI asset inventory + data flow. Risk register with owners, dates, closure evidence. |
| 02 | **Sanction Policy** | §164.308(a)(1)(ii)(C); §164.530(e) | Written tiered sanction policy. Signed workforce acknowledgments. Evidence it has actually been applied. |
| 03 | **Audit, Logging & Activity Review Policy** | §164.308(a)(1)(ii)(D); §164.312(b) | Documented log-review cadence. Named reviewer. Dated sign-offs. Log retention standard. |
| 04 | **Workforce Security Policy** | §164.308(a)(3) | Authorization & supervision procedures. Clearance / background screening. Termination deprovisioning tickets with timestamps. |
| 05 | **Access Control Policy** | §164.308(a)(4); §164.312(a), (d) | Unique user IDs — no shared logins. Break-glass emergency access procedure. Periodic access recertification. |
| 06 | **Security Awareness & Training Policy** | §164.308(a)(5); §164.530(b) | Curriculum. Completion roster including management. Periodic security reminders. Password & malware procedures. |
| 07 | **Security Incident Response Policy** | §164.308(a)(6) | IR plan. Log of ALL security incidents — not just breaches. Tabletop exercise after-action reports. |
| 08 | **Breach Notification Policy** | §164.400–414 | Four-factor risk assessment on every impermissible disclosure. Notice templates. HHS portal submissions. 60-day clock. |
| 09 | **Contingency Planning Policy** | §164.308(a)(7) | Data backup plan. Disaster recovery plan. Emergency mode operation plan. BIA with RTO/RPO. Documented restore test. |
| 10 | **Business Associate Management Policy** | §164.308(b); §164.314(a); §164.502(e) | Complete BA inventory. Executed BAAs with subcontractor flow-down and §164.410 breach-reporting clauses. |
| 11 | **Facility & Workstation Security Policy** | §164.310(a), (b), (c) | Facility security plan. Visitor control log. Maintenance records. Workstation use standard covering remote work. |
| 12 | **Device & Media Control Policy** | §164.310(d) | Media disposal & re-use procedures per NIST SP 800-88. Certificates of destruction. Chain-of-custody log. |
| 13 | **Data Integrity & Transmission Security Policy** | §164.312(c), (e) | Encryption standard — at rest and in transit. Integrity monitoring. TLS enforcement. Triggers the breach safe harbor. |

| **18** | **36** | **22** | **6** |
|---|---|---|---|
| **standards** | **implementation specs** | **Addressable, not optional** | **years retention** |
| 9 admin · 4 physical · 5 technical | 14 Required · 22 Addressable | §164.306(d)(3) | §164.316(b)(2)(i) |

### WHAT MOST PRACTICES ACTUALLY HAVE

Training records. Maybe a BAA folder. Occasionally an old risk assessment the EHR vendor ran once. That is **three of fourteen.**

The single most-cited deficiency in OCR investigations is **§164.308(a)(1)(ii)(A) — Risk Analysis.** A checklist review of your policies is not a risk analysis. A vendor questionnaire is not a risk analysis.

In 2026 OCR formally expanded that initiative to include **§164.308(a)(1)(ii)(B) — Risk Management:** what you actually did about what you found.

**Encryption of ePHI at rest and in transit is the single highest-leverage control.** Done to HHS specification, it removes the breach-notification obligation entirely.

### WHAT IT COSTS TO BE WRONG

Civil monetary penalties, inflation-adjusted effective **January 28, 2026** (OMB multiplier 1.02598).

| TIER | CULPABILITY | PER VIOLATION | CAL-YR CAP |
|---|---|---|---|
| 1 | Did not know | $145 – $73,011 | $2,190,294* |
| 2 | Reasonable cause | $1,461 – $73,011 | $2,190,294* |
| 3 | Willful neglect, corrected | $14,602 – $73,011 | $2,190,294* |
| 4 | **Willful neglect, uncorrected** | **$73,011 – $2,190,294** | **$2,190,294** |

* OCR's April 2019 Notice of Enforcement Discretion applies substantially lower calendar-year caps to Tiers 1–3. It has never been rescinded, and the Federal Register schedule does not reflect it.

**And the multiplier:** under **§160.406**, a continuing violation is a **separate violation for every day it persists.** An unencrypted server is not one violation. It is one violation per day, per requirement.

**Count how many of these 14 you have.** Most practices stop at three.

Book a free 30-minute Compliance Reality Check. We will walk your gaps line by line — no obligation, no pitch deck.

**dspcybersecurity.com** · Bradenton · Sarasota · Tampa Bay · CISM, CISA, CRISC