HIPAA Product-Team Cheat Sheet

The three rules, the role test, the 2026 penalties, and the 60-day clock - on one page.

THE THREE RULES (45 CFR 160, 164)

Privacy Rule (2003) - who may see PHI
Default deny (s.164.502). Minimum-necessary access. Patient rights: export records within 30 days (s.164.524). For a BA, the BAA sets the permitted uses.

Security Rule (2005) - how ePHI is protected
Documented risk analysis (s.164.308). Admin + physical + technical safeguards (s.164.312): access control, audit logs, integrity, authentication, transmission security. Technology-neutral.

Breach Rule (2009) - when protection fails
Breach presumed unless a documented 4-factor assessment shows low probability of compromise. Encrypted data whose key did not leak = not reportable.

WHICH ONE ARE YOU? (s.160.103)

Business associate (most product teams)
You create, receive, maintain, or transmit PHI for a provider, plan, or clearinghouse - or for their vendor (subcontractor BA). BAA required; direct liability since 2013.

Covered entity
You deliver or pay for care: the medical group of a DTC telehealth service, a clinic, a plan. All three rules in full.

Neither - FTC territory
Consumers picked your app independently; no covered entity directs you. FTC Health Breach Notification Rule (16 CFR 318) applies instead.

THE 60-DAY BREACH CLOCK

Discovery Mar 3 -> notices by May 2
28 days left in March + 30 in April + 2 in May = day 60. Individuals: within 60 days (s.164.404). 500+: HHS + media at once (s.164.406-408). BA -> CE: 60-day max, BAAs often say 5-10 days (s.164.410).

Pre-write the runbook
Four-factor assessment template, notice templates, contact tree - before launch, not after discovery.

2026 CIVIL PENALTIES (eff. 2026-01-28)

Tier 1 - no knowledge	$145 - $73,011 per violation
Tier 2 - reasonable cause	$1,461 - $73,011 per violation
Tier 3 - willful neglect, corrected <=30d	$14,602 - $73,011 per violation
Tier 4 - willful neglect, uncorrected	$73,011 - $2,190,294 per violation

Annual cap $2,190,294 per provision. Criminal track (42 U.S.C. 1320d-6): up to $250,000 and 10 years. OCR's Risk Analysis Initiative: the first artifact requested is your risk analysis.

THE EIGHT STEPS

- [ ] **Classify yourself** — covered entity, business associate, or neither
- [ ] **Map the PHI** — every system, vendor, log, and backup it can reach
- [ ] **Risk analysis, documented** — s.164.308(a)(1)(ii)(A) - keep it current
- [ ] **Close the BAA chain** — signed BAA on every hop; no BAA = no PHI
- [ ] **Implement safeguards** — encryption in transit + at rest, MFA, RBAC, audit log, timeouts
- [ ] **Privacy Rule surface** — min-necessary access, 30-day export, authorizations beyond TPO
- [ ] **Breach playbook** — 4-factor template + notice drafts; 60-day clock marked
- [ ] **Train and document** — policies, training, sanctions; keep records 6 years (s.164.316)

Remember: encrypted is not compliant, available is not configured, and a 'HIPAA Certified' badge has no legal meaning. Engineering guidance, not legal advice.

Companion to: 'HIPAA in Plain English for Product Teams'
www.forasoft.com/learn/telemedicine/articles-telemedicine/hipaa-for-telemedicine-product-teams



GO DEEPER · THE 7-VOLUME HANDBOOK

Fora Soft Video Engineering Handbook

Seven volumes, 9,000+ pages: encoding, streaming, audio and AI for video products — from the pixel to production.

By Nikolay Sapunov, CEO at Fora Soft · Kindle & paperback on Amazon

Browse the handbook on Amazon →

This sheet puts the three HIPAA rules, the role test, the 2026 penalty tiers and the breach clock in front of a product team. Our seven-volume handbook covers the video stack those rules apply to; start with Volume 7 for compliance and serving, then Volume 3 for WebRTC and DRM.

WHAT YOU WILL FIND INSIDE

- Compliance and regulated AI (Vol. 7)
- WebRTC and real-time delivery (Vol. 3)
- AI inside real-time calls (Vol. 7)
- DRM and protected playback (Vol. 3)

THE FULL HANDBOOK · 7 VOLUMES · 9,000+ PAGES · ALL ON AMAZON

Vol. 1 · Video Encoding — pixels and color to H.264, HEVC, AV1, quality metrics and AI

Vol. 2 · Video Streaming I — network transport, contribution and ingest, HLS, MPEG-DASH, CMAF

Vol. 3 · Video Streaming II — ABR, CDNs, players, WebRTC, DRM and the economics of delivery

Vol. 4 · Audio for Video I — PCM, codecs, loudness, accessibility, real-time voice processing

Vol. 5 · Audio for Video II — jitter buffers, lip sync, Atmos, quality metrics, neural codecs

Vol. 6 · AI for Video I — models and inference, computer vision, speech, search, generative video

Vol. 7 · AI for Video II — real-time pipelines, agents, serving, cost, compliance, verticals

Building a telehealth product and unsure whether you are a business associate?

We will map your PHI flows, check the BAA chain and safeguards against the rules, and give you the eight-step plan with owners. 250+ video products shipped since 2005.

Book a 30-min call → **WhatsApp →** **Email us →**