

HIPAA 2026 Migration Checklist for Video Platforms

The proposed Security Rule change set (90 FR 898, Jan 6, 2025) mapped to a telemedicine video stack. Check what you already have; the gaps are your backlog.

KNOW YOUR ESTATE — prop. §164.308(a)(1)-(2)

- Written asset inventory covers signaling, TURN, SFU, recording nodes, transcripts, and every vendor
- ePHI network map is ≤ 12 months old and shows where media is decrypted (SFU) and where it is relayed (TURN)
- Risk analysis starts from the inventory and assigns a risk level to each threat-vulnerability pair

KEEP CHECKING — prop. §164.308(a)(4), §164.312(d), (h)

- Vulnerability scans every 6 months include TURN and SFU nodes, not just the web tier
- Penetration test completed within the last 12 months
- Patch path proven: critical ≤ 15 / high ≤ 30 calendar days; media fleet rotates without dropping consults
- Audit trail answers who accessed which session, when, from where — and is exportable

PROVE IT ANNUALLY — prop. §164.308(a)(14), (b)

- Annual Security Rule self-audit is on the calendar with a named owner
- SME-verified written safeguards analysis ready to hand to covered-entity customers
- Annual verifications collected from every ePHI-touching vendor (cloud, media, transcription)

HARDEN BY DEFAULT — prop. §164.312(b), (c), (f)

- Recordings, transcripts, chat, attachments, and backups encrypted at rest; signed URLs expire
- MFA on patient, provider, admin, cloud-console, and CI/CD logins — patient UX designed, not bolted on
- Media plane, control plane, and data plane sit in segmented network zones
- Consistent baselines: anti-malware, extraneous software removed, unused ports disabled

SURVIVE THE HIT — prop. §164.308(a)(13), §164.312(i)-(j)

- Documented, tested 72-hour restore for consult-critical systems (signaling, media, schedule)
- Criticality ranking exists: tomorrow's consults outrank last month's archive
- Exact backups under separate technical controls; 24-hour customer-notice page in the incident runbook

Status: proposed rule as of 2026-06-11 — no final rule published. Once final: effective +60 days, compliance +180 more (≈ 240 total). Verify status at [federalregister.gov](https://www.federalregister.gov), RIN 0945-AA22.

THE ANNUAL CADENCE UNDER THE PROPOSAL — put owners and dates on each

With six ePHI-touching vendors: 2 vulnerability scans + 1 penetration test + 1 compliance audit + 1 risk-analysis refresh + 1 inventory & map refresh + 1 incident-response plan test + 6 vendor verifications collected + 1 verification produced for your customers = 13 scheduled compliance events a year.