EMRY NETWORKS
IT Solutions That Click

2026 HEALTHCARE & DENTAL COMPLIANCE GUIDE • HIPAA SECURITY RULE & PROPOSED NPRM

Dental & Medical Practice HIPAA Security Rule & Third-Party Portal Checklist

10 Essential Technical Safeguards to Defeat 29-Minute eCrime Breakouts, Secure 3D CBCT/EHR Workloads, and Pass HHS OCR Audits.

45 CFR 164.308 / 164.312 • BAA • PCI DSS 4.0.1

< 15 Min	4 Minutes	100% VLAN	Signed BAA
Chairside PMS & Imaging Failover	24/7 SOC Host & Token Isolation	CBCT, EHR & Payment Isolation	Live Auditor Evidence Binder

WHAT'S INSIDE

- How to use this checklist and assessment details — p. 2
- 1 The 10 controls: status, owner, target date and evidence — p. 3
- 2 Your results and open items — p. 5
- Rules cited, related resources and next step — p. 6

Book a 30-Minute Risk Assessment →

USING THE INTERACTIVE VERSION

- **Type in any shaded box.** Press Tab to move to the next one.
- **Blue-outlined boxes are drop-downs** for each control's status.
- **Grey boxes calculate themselves:** the counts, readiness % and open items on your Results page.
- **Best in Adobe Acrobat Reader (free)** or another desktop PDF app. Browser viewers and Apple Preview let you type, but may not run the calculations; you can type those values in yourself.
- **Use the links** in the contents list, the header (Contents, Results) and the bookmarks panel to jump around.
- **Save often.** Prints on US Letter, landscape; the on-screen buttons do not print.

Print checklist | Clear all entries

STATUS KEY

In place: Implemented today and you can show evidence. Earns all of the control's points.
Partial: Started, or covers only some users, systems or sites. Earns 40% of the control's points.
Gap: Not in place yet. Earns 0 points, the same as a control you have not marked.
N/A: Does not apply to your practice. Offered only on controls 04 and 08, and left out of the readiness %.

How to use this checklist

45 CFR 164.308 / 164.312

1. Mark a status for each control. Use the drop-down next to each of the 10 controls: In place, Partial or Gap (N/A only where it is offered).

2. Assign the work. For anything Partial or a Gap, name an owner and a target date.

3. Note the evidence. Say where the proof lives (policy, screenshot, report, contract), so you can produce it on request.

4. Review your results. The Results page counts your answers, works out a weighted, self-rated readiness % and lists the open items.

5. Get a second opinion. Bring the results to a 30-minute risk assessment if you want an outside review.

Assessment details

Practice / legal entity		**Date completed**	
Completed by (name, title)		**Next review date**	
Locations in scope (all sites)		**Security official (164.308(a)(2))**	

The controls at a glance

01 Live-System HIPAA Security Risk Analysis (45 CFR 164.308(a)(1)(ii)(A))
02 Third-Party Clinical & Lab Portal Access Governance (Quest Quanum / Change Healthcare)
03 FIDO2 Phishing-Resistant MFA on Email & Password-Reset Inboxes
04 Strict VLAN Micro-Segmentation for CBCT Imaging, Sensors & IoMT
05 Sub-15-Minute Chairside PMS/EHR BCDR Failover (Proposed 72-Hour Restore Rule)
06 4-Minute 24/7 MDR Endpoint & Identity Containment
07 Signed HIPAA Business Associate Agreements (BAAs) & Vendor Matrix
08 PCI DSS 4.0.1 Cardholder Data Environment (CDE) Isolation
09 365-Day Immutable Audit Logs & ePHI Export Telemetry (45 CFR 164.312(b))
10 Annual Clinical Incident Response Tabletop & Workforce Phishing Drills

Disclaimer

This checklist is an educational self-check, not legal advice, a certification, or a formal assessment. Confirm requirements against the current regulation, your contracts, and your assessor or counsel. © 2026 Emry Networks.

1 The 10 controls

45 CFR 164.308 / 164.312

For each control, pick a status, then add an owner, a target date and where the evidence lives. Your answers feed the Results page.

01. Live-System HIPAA Security Risk Analysis (45 CFR 164.308(a)(1)(ii)(A))

Maintain a continuously updated asset inventory and risk register covering every operatory PC, EHR server, imaging sensor, and cloud portal touching ePHI.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

02. Third-Party Clinical & Lab Portal Access Governance (Quest Quanum / Change Healthcare)

Eliminate shared front-desk logins, purge former employees within 0 minutes, and log quarterly access reviews for lab, clearinghouse, and referral portals.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

03. FIDO2 Phishing-Resistant MFA on Email & Password-Reset Inboxes

Protect Microsoft 365 / Google Workspace mailboxes that receive lab and EHR password-reset links against AiTM session-token replay attacks.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

04. Strict VLAN Micro-Segmentation for CBCT Imaging, Sensors & IoMT

Isolate Dexis, Planmeca, Carestream 3D CBCT, DICOM/PACS, and operatory X-ray workstations from front-desk payment terminals and patient guest Wi-Fi.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

05. Sub-15-Minute Chairside PMS/EHR BCDR Failover (Proposed 72-Hour Restore Rule)

Ensure Dentrix, Eaglesoft, Open Dental, eClinicalWorks, or athenahealth workloads fail over in <15 minutes with quarterly verified restoration certificates. The 72-hour restoration requirement is proposed in HHS's January 2025 Security Rule NPRM and is not yet final; today's rule already requires a contingency plan (45 CFR 164.308(a)(7)).

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

06. 4-Minute 24/7 MDR Endpoint & Identity Containment

Monitor all clinical endpoints 24/7/365 with human-led SOC engineers and behavioral canary traps that isolate ransomware staging in under 4 minutes.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

07. Signed HIPAA Business Associate Agreements (BAAs) & Vendor Matrix

Maintain executed HIPAA BAAs and 72-hour breach notification SLAs with your MSP/MSSP, cloud backup provider, VoIP vendor, and imaging contractors.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

08. PCI DSS 4.0.1 Cardholder Data Environment (CDE) Isolation

Segment patient credit-card and HSA/FSA payment terminals onto a dedicated PCI VLAN with zero connectivity to clinical ePHI databases.

STATUS · 1 PT | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

09. 365-Day Immutable Audit Logs & ePHI Export Telemetry (45 CFR 164.312(b))

Retain tamper-proof audit trails tracking every bulk patient report export, login anomaly, and privilege escalation across PMS and EHR databases.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

10. Annual Clinical Incident Response Tabletop & Workforce Phishing Drills

Execute and document annual ransomware/portal-breach tabletop exercises for practice managers and providers to satisfy OCR good-faith enforcement criteria.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

2 Your results and open items

Calculated from the 10 controls

These totals fill in automatically from your answers in Adobe Acrobat Reader and most desktop PDF apps. If a box stays blank in your viewer, count from the controls pages and type or write the number in. Readiness is your own self-assessment, not a compliance determination.

In place	Partial	Gap	N/A	Assessed (controls marked)	Readiness (self-rated)	Gaps and partials with no owner

Points:

Readiness = points earned ÷ points available. Each control is worth 5, 3 or 1 points (shown next to its status). In place earns all of its points, Partial earns 40%, and a Gap or an unmarked control earns 0, so the score climbs from 0% as you mark controls. N/A controls are left out of the points available.

Open items to close (calculated: Gaps first, then Partials, with owner and target date)

Sign-off

Reviewed by (name, title)	
Signature / date	
Date of next review	

Rules and documents cited in this checklist

Official sources for the rules, standards and documents named in the controls above. Check them for updates before relying on any requirement.

45 CFR 164.308 Administrative safeguards (eCFR): https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.312 Technical safeguards (eCFR): https://www.ecfr.gov/current/title-45/section-164.312
Federal Register: Proposed HIPAA Security Rule changes (NPRM, Jan 6, 2025):
https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
PCI Security Standards Council: PCI DSS v4.0.1: https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1

Sources for the figures on the cover

29-minute breakouts: Average eCrime breakout time in 2025 was 29 minutes (CrowdStrike 2026 Global Threat Report, Feb. 24, 2026).
https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
Proposed NPRM / 72-hour restore: HHS NPRM, 90 FR 898 (Jan. 6, 2025) is still a proposed rule; the Unified Agenda lists final action for 07/2027 (RIN 0945-AA22).
https://www.reginfo.gov/public/do/eAgendaViewRule?RIN=0945-AA22&pubId=202510
Contingency plan: 45 CFR 164.308(a)(7) contingency plan standard (current rule). https://www.ecfr.gov/current/title-45/section-164.308#p-164.308(a)(7)

Related Emry Networks resources

HIPAA Security Checklist for Dental & Medical Practices (web page): https://www.emrynetworks.com/hipaa-security-checklist-dental-medical
HIPAA Risk Analysis Lessons From an $800,000 Settlement: https://www.emrynetworks.com/post/hipaa-risk-analysis-audit-log-review-medical-groups
IT security for dental practices: https://www.emrynetworks.com/services/regulated-industries/dental-practices
IT security for medical practices: https://www.emrynetworks.com/services/regulated-industries/medical-practices
HIPAA compliance services: https://www.emrynetworks.com/services/regulated-industries/hipaa

Want a second set of eyes on your HIPAA safeguards?

Emry Networks helps dental and medical practices put these safeguards in place and keep the evidence an auditor will ask for. Call (603) 202-3200 or Book a 30-Minute Risk Assessment.

EMRY NETWORKS • DEFENSIBLE IT, 24/7 MDR & LIVE COMPLIANCE ENGINEERING
Jacksonville, FL & Manchester, NH Operations Hubs • Serving Regulated SMBs Across All 50 States • (603) 202-3200 • www.emrynetworks.com/contact-us

Book a 30-Minute Risk Assessment →

Print checklist
Clear all entries