

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

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

< 15 Min

Chairside PMS & Imaging Failover

4 Minutes

24/7 SOC Host & Token Isolation

100% VLAN

CBCT, EHR & Payment Isolation

Signed BAA

Live Auditor Evidence Binder



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

Ensure Dentrix, Eaglesoft, Open Dental, eClinicalWorks, or athenahealth workloads fail over in <15 minutes with quarterly verified restoration certificates.



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



08. PCI DSS 4.0 Cardholder Data Environment (CDE) Isolation

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



10. Annual Clinical Incident Response Tabletop & Workforce Phishing Drills

[] PASS [] GAP / REMEDIATE

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