SAMPLE - FULL HIPAA AUDIT - $99

HIPAA Readiness *Audit Report.*

Prepared for: Sample Dental Practice
Prepared by: CyberDental Group LLC
Report date: May 12, 2026

This sample demonstrates the structure, evidence categories, risk scoring, remediation roadmap, and certification blocks included in the CyberDental HIPAA audit deliverable. Final reports are issued only after practice review and credential verification.

Overall Status	Risk Level	Priority Items
Readiness Review	Moderate Sample	12 Findings

EXECUTIVE SUMMARY

What the audit provides.

CyberDental reviews administrative, physical, and technical safeguard readiness for dental practices that create, receive, maintain, or transmit electronic protected health information (ePHI). The audit is designed to identify practical gaps before they become violations, breaches, costly fines, or operational disruption.

This sample report uses simulated findings. A final report includes practice-specific evidence, documented recommendations, and signature blocks for the HIPAA Officer and CyberDental executive attestation.

AUDIT SCOPE

Everything the audit reviews.

Area	What Is Audited	Sample Risk
Risk Analysis	ePHI inventory, threats, vulnerabilities, likelihood, impact, and priority risks.	High
Policies & Procedures	Privacy, security, breach, backup, device, access, and vendor documentation.	Moderate
Encrypted Email	Secure transmission workflows for patient data and sensitive attachments.	Moderate
Cloud Backup	Backup frequency, restore readiness, disaster recovery, and emergency operations.	High
Endpoint Protection	Workstations, laptops, patching, anti-malware/EDR, device control, and monitoring.	Moderate
HIPAA Training	Workforce training evidence, role-based procedures, sanctions, and phishing awareness.	Low
Firewall & Network	Remote access, traffic filtering, Wi-Fi separation, router configuration, and logging.	High
Pentesting Readiness	External exposure, periodic technical evaluation planning, and remediation proof.	Moderate
Vendors & BAAs	Business associate agreements for IT, cloud, email, billing, imaging, and support vendors.	Moderate
Incident Response	Security incident procedure, escalation, documentation, containment, and continuity workflow.	Moderate

PREVENTION

What the audit helps prevent.

HIPAA violations

Find missing documentation, weak safeguards, and unmanaged workflows before compliance exposure.

Patient breaches

Reduce unauthorized access, unencrypted transmission, compromi-sed

Costly fines

Create evidence that risks are reviewed and reasonable safeguards are planned and tracked.

Business discontinuity

Validate backup, restore, emergency operation, and response workflows before outages stop care.

EVIDENCE CHECKLIST

Documents and proof reviewed.

Evidence Requested	Purpose
Policies and procedures	Administrative documentation and office expectations.
Training records	Workforce education and role-based awareness.
Backup logs and restore proof	Continuity planning and recoverability.
Firewall/router summary	Network protections, remote access, segmentation.
Endpoint security status	Device protection, patch posture, malware defenses.
Vendor list and BAAs	Third-party ePHI handling and contractual safeguards.
Incident response plan	Containment, documentation, notification, escalation.

SAMPLE FINDINGS

Priority snapshot.

Finding	Priority	Recommended Action
No documented annual security risk analysis provided.	High	Complete written risk analysis with owners.
Backup restore test evidence was not available.	High	Run restore validation and keep dated proof.
Remote access policy did not define MFA/vendor revie-w.	Moderate	Require MFA, named users, logs, quarterly review.
Workforce HIPAA training records were incomplete.	Moderate	Complete annual training and signed acknowledgements.

REMEDIATION ROADMAP

Action plan after the audit.

Timeline	Action
0-7 days	Approve audit findings, assign owners, and secure missing policy/training evidence.
7-30 days	Implement MFA, review vendor access, validate backups, and document restore testing.
30-60 days	Complete firewall review, endpoint remediation, email encryption workflow, and BAA cleanup.
Quarterly	Review access logs, patch status, vendor list, backup proof, and security incidents.
Annual	Refresh risk analysis, training, policies, technical evaluations, and executive sign-off.

CERTIFICATION BLOCKS

Sample signatures.

The final report is certified after CyberDental completes the practice review. License details must be verified before final issuance. The signatures below are displayed as sample typed signatures for report layout review.

Monica Guerrero

HIPAA Officer

License No.: SAMPLE-LIC-0000
Replace with verified license number before final report issuance.

Dimitri Lopez

CEO & Founder

CyberDental Group LLC
Executive attestation on CyberDental's behalf.

SAMPLE ONLY - FINAL REPORT REQUIRES VERIFIED PRACTICE REVIEW

This sample is not legal advice, a final HIPAA certification, or a guarantee against enforcement action. It is an example of the CyberDental HIPAA audit report format and remediation workflow.