September 10
gocorptech.com

CORPORATE TECHNOLOGIES LLC

# Beyond HIPAA: A Holistic Compliance Checklist for Dental IT

**Published by Corporate Technologies, Eden Prairie, MN**

# Executive summary

Modern dental practices have evolved into highly digital environments, often with complex technology stacks supporting everything from imaging to billing. While most are familiar with HIPAA, many practice owners fall into the "HIPAA-only fallacy" — believing that compliance begins and ends there. In reality, PCI DSS, the FTC Safeguards Rule, and the 21st Century Cures Act also impose serious obligations, and the risks of non-compliance range from fines to reputational damage to outright business disruption.

This white paper cuts through the complexity by walking you through each major compliance domain and offering an actionable 90-day checklist to help you close your most critical gaps. Whether you're managing your own IT or working with a partner, you'll learn exactly where your risks lie — and how GoCorpTech can help you address them efficiently.

## Key takeaways

- HIPAA is just the beginning. You need to understand the full landscape of compliance risks.
- Federal rules like PCI DSS 4.0 and the FTC Safeguards Rule now apply to many dental offices.
- Simple tools like MFA, encryption, and vendor checklists can dramatically reduce risk.
- GoCorpTech helps small practices implement the same best practices that insurers and large DSOs expect.

# Introduction

Modern dental practices are tech-driven businesses first and clinics second. Nearly every office in the U.S. now runs on electronic health records, digital radiographs, intraoral scanners, cloud-based practice management platforms, teledentistry tools, and online payment systems. These digital systems bring efficiency and new opportunities to serve patients, but they also bring risk. Every tool touches a different compliance domain, creating multiple obligations for practice owners.

Unfortunately, many fall into what we call a HIPAA-only fallacy: The belief that HIPAA is the beginning and end of compliance in dentistry. In reality, HIPAA is just one piece of a much larger puzzle. A credit card terminal, for example, brings PCI DSS into play, while a patient financing program triggers the FTC Safeguards Rule, and the 21st Century Cures Act requires timely patient access to electronic records. Crucially, the rapid move to cloud-based platforms means your practice's risk is now tied directly to your vendors' security posture.

# Case in Point

## Aspen Dental Breach

### What happened:

In 2023, Aspen Dental — one of the largest dental chains in the U.S. — was hit by a devastating ransomware attack.

### The impact:

- Patient records and scheduling systems were offline for weeks.
- More than 1,000 locations were affected nationwide.
- Emergency care and business operations ground to a halt.

### Why it matters to you:

If a billion-dollar DSO with dedicated IT teams can be paralyzed by a breach, imagine what the fallout would look like for a small, independent practice. A similar attack could mean:

- Lost chair time and canceled appointments.
- Permanent reputation damage.
- Patients who never return.
- Regulatory fines and insurer denials if security basics weren't in place.

**Don't assume you're too small to be a target.** Threat actors don't discriminate: they look for vulnerable systems, not brand names.

# Non-compliance has serious consequences

The consequences of overlooking your compliance obligations — even accidentally — are painfully real. In recent years, dental practices have been fined for a range of infractions, from mishandling patient data on Yelp ($23,000) to delaying patient access to records ($80,000). Westend Dental was fined a staggering $350,000 in 2025 for failing to report a ransomware attack and storing passwords in plain-text documents.

These examples are relatively tame in comparison to what's theoretically possible. For example, fines for PCI noncompliance can reach $100,000 per month, and in some cases, payment processors revoke the ability to accept card payments altogether.

But financial losses are just one factor. A breach or system outage means lost chair time, disrupted scheduling, and reputational harm that lingers long after the systems come back online. When Aspen Dental was hit with a ransomware attack in 2023, its scheduling and patient records were unavailable across more than 1,000 locations for weeks.

For a small practice, an incident like this could be existential due to reputational damage and loss of trust. Patients who lose confidence in your ability to protect their data may not return, and insurers are increasingly denying claims if basic safeguards like multi-factor authentication and encryption aren't verifiably in place.

This white paper is designed to help practice owners cut through the complexity. We'll walk through the key compliance domains beyond HIPAA and provide a holistic checklist that can serve as a starting point for a self-audit. By the end, you'll have a clear view of where the gaps might be in your practice and how to address them before they snowball.

# A non-negotiable foundation

Although HIPAA by itself isn't sufficient, it remains the foundation of compliance for dental practices. Any office that transmits health information electronically — from submitting claims to verifying patient eligibility — falls under the HIPAA Privacy, Security, and Breach Notification Rules. These rules govern how PHI must be stored, transmitted, and disclosed, and violations carry significant penalties.

For years, HIPAA allowed some flexibility through so-called "addressable" safeguards. That flexibility is shrinking. In January 2025, regulators proposed updates to the HIPAA Security Rule that, once finalized, will shift several key technical safeguards from "addressable" to mandatory.

# *Some of the new mandates rules under the 2025 Security Rule update include:*

**Multi-factor authentication (MFA)**

MFA becomes mandatory for all systems accessing ePHI. Temporary exceptions may apply to unsupported legacy devices, provided there's a formal migration plan.

**Network mapping**

Practices must maintain an up-to-date, written inventory of all technology and media handling ePHI, plus a detailed network map showing how PHI flows through their environment.

**Formal incident response and disaster recovery**

Practices must develop formal, documented plans for responding to breaches or outages, including clearly defined roles. These plans must be tested at least once a year.

**Mandatory encryption at rest and in transit**

All ePHI must be encrypted, including data on servers, in backups, and when transmitted via email or portals, aligned with current cryptographic standards.

**What does this mean for you?** It means running a busy, patient-focused practice while managing increasingly complex tech safeguards, and doing it without cutting corners.

# HIPAA Essentials Checklist

**Make sure you can say "yes" to all:**

- [ ] MFA is enabled for all logins that access ePHI.
- [ ] All ePHI is encrypted at rest (servers, databases, laptops, cloud).
- [ ] All ePHI is encrypted in transit (email, patient portals, remote access).
- [ ] Annual HIPAA risk analysis conducted and documented.
- [ ] Network map updated to show all devices handling ePHI.
- [ ] Incident response and disaster recovery plan.
    - [ ] Written and tested within the last 12 months.
- [ ] Staff training is completed annually on HIPAA and security basics.

**Need help getting these basics in place?** GoCorpTech can audit your current HIPAA posture and implement safeguards aligned with the 2025 rule changes.

# Beyond HIPAA: Other federal requirements

HIPAA may be the foundation, but it is not the only federal rulebook dental practices must follow. Other regulations come into play the moment you swipe a patient's credit card, offer financing, or provide electronic access to records. Overlooking these requirements can create just as much risk as a HIPAA violation (and sometimes more!)

## PCI DSS 4.0 for credit card security

Any dental practice that accepts card payments is subject to the Payment Card Industry Data Security Standard (PCI DSS). Version 4.0 became mandatory in March 2025 and brings stricter requirements for protecting cardholder data. For practices, this means segmenting the payment environment from the rest of the office network, enforcing MFA on payment systems, and conducting quarterly vulnerability scans to identify weaknesses. Noncompliance can result in fines of up to $100,000 per month and, in severe cases, the loss of card-processing privileges altogether.

### Quick fact

PCI DSS 4.0 isn't just for big retailers. Any dental practice that accepts even a single credit card transaction is in scope. Processors **will** revoke your ability to take card payments if you're not compliant.

## FTC Safeguards Rule for financing and credit

If your practice offers patient financing or credit, the FTC considers you a "financial institution" under the Gramm-Leach-Bliley Act. That designation brings additional responsibilities. The Safeguards Rule requires you to maintain a written information security program, designate a qualified security lead, and encrypt financial data. You must also conduct regular risk assessments and train staff to follow your policies. Ignoring these requirements can expose practices not only to regulatory action and lawsuits.

## 21st Century Cures Act for patient access

The Cures Act ensures patients have a legal right to prompt, electronic access to their complete health records. In practical terms, this means your EHR or patient portal must allow patients to view, download, and share their records without unnecessary delays or fees. Blocking or delaying access (even unintentionally) can be considered "information blocking" under the law and lead to enforcement action. For dental practices, compliance requires both the right technology and the right workflows to support timely record sharing.

# Federal compliance checklist

- [ ] Quarterly PCI vulnerability scans performed and documented.
- [ ] Credit card processing network segmented from clinical/office network.
- [ ] MFA enabled on all payment systems.
- [ ] Patient financing/credit data encrypted and written security program documented.
- [ ] Qualified individual designated to oversee the Safeguards Rule program.
- [ ] Patients can securely access their complete records electronically.
- [ ] Policies in place to prevent information blocking and ensure timely record release.

**Feeling overwhelmed? You're not alone.** GoCorpTech can manage your PCI, FTC, and Cures Act obligations, so you can stay focused on patients.

# International standards influencing U.S. dentistry

Beyond federal rules, there's a set of industry and international frameworks shaping how dental IT gets built, bought, and audited. While not always legally required, they're frequently referenced by HHS, expected by insurers, and requested by larger groups/DSOs and vendors during due diligence. Aligning with them future-proofs your practice and reduces vendor risk.

## ISO 27001 & 27799

ISO/IEC 27001 is the global benchmark for building an information security management system (ISMS). Healthcare organizations use 27001 to demonstrate disciplined, auditable security, and many rely on it to show "good-faith" alignment with HIPAA's Security Rule. Meanwhile, ISO 27799 tailors ISO controls to health data specifically (how to select, implement, and manage safeguards for PHI across systems and workflows).

## ADA/ANSI standards for AI in dentistry

In 2025, the ADA published the first U.S. standard for AI in dentistry: ANSI/ADA 1110-1:2025, which sets criteria for how dental radiographs are annotated and collected so AI tools can be validated and used safely in clinical decision-making. If your practice is evaluating AI-powered radiograph analysis, vendors should be able to speak to this standard.

## NIST Cybersecurity Framework

HHS and industry bodies point providers to NIST CSF as a practical blueprint for managing cyber risk (Identify → Protect → Detect → Respond → Recover). HHS has even published a HIPAA–NIST CSF crosswalk, and NIST's 2024 update to SP 800-66 provides fresh mappings between HIPAA Security Rule requirements and the CSF/800-53 controls. Insurers increasingly reference these same control families in underwriting questionnaires.

### Quick fact

HHS released an official HIPAA↔NIST CSF crosswalk to help providers operationalize HIPAA using NIST language.

## Aligning with international standards (quick wins)

**Vendor contracts**

Vendors handling PHI/financial data have BAAs or equivalent security terms in place.

**Security frameworks**

Key vendors can demonstrate alignment with ISO 27001/27799 or NIST CSF practices (e.g., policies, risk assessments, access controls, backups.)

**AI due diligence**

Any AI-based dental tool (e.g., radiograph analysis) is evaluated against ANSI/ADA 1110-1:2025 (data/annotation/validation practices.)

**Policy hygiene**

Practice IT/security policies are reviewed annually against NIST categories.

# You don’t need to do this alone.

GoCorpTech helps you vet vendors, align policies with NIST, and build trust with insurers.

# A consolidated compliance checklist for dentists

**HIPAA: Security Rule must-haves**

- [ ] Annual risk analysis documented and remediations tracked.
- [ ] Contingency plans with tested backups and disaster recovery.
- [ ] Encryption for ePHI in transit and at rest; MFA on systems that access ePHI.
- [ ] Up-to-date asset inventory and/or network map for ePHI systems.

**PCI DSS 4.0: If you take cards**

- [ ] Quarterly external ASV vulnerability scans (and rescans as needed.)
- [ ] Network segmentation that isolates cardholder data from clinical systems.
- [ ] MFA for all access into the CDE (required as of March 2025.)
- [ ] All policies updated to PCI DSS v4.0; future-dated controls met.

**FTC Safeguards Rule: If you offer financing or credit**

- [ ] Encryption of customer financial data; vendor oversight and staff training.
- [ ] Breach reporting to FTC within 30 days for incidents affecting ≥500 consumers.
- [ ] Written information security profile; qualified individual designated, periodic assessments.

**21st Century Cares Act: For patient electronic access**

- [ ] Patients can view/download/share EHI electronically without delay.
- [ ] Staff know the limited exceptions and how to fulfill requests promptly.
- [ ] Understand potential penalties for information blocking.

# Your action plan for compliance

**Days 0 - 30**

1 Run a HIPAA risk analysis and capture gaps. Verify backups and DR drill dates.

2 Confirm PCI scope (if applicable), isolate the CDE, and schedule quarterly scans.

3 If you offer financing, appoint a Safeguards Rule lead and draft a WISP outline.

4 Validate patient portal/EHR workflows for Cures Act access; document exceptions process.

**Days 31 - 60**

5 Enable MFA everywhere it’s requred (ePHI systems; all access into the CDE.)

6 Turn on and verify encryption across servers, laptops, cloud, and remote access.

7 Update BAAs and vendor questionnaires to include NIST/ISO expectations and Cures Act support.

**Days 61 - 90**

**8** Test DR/IR playbooks and record results; fix findings.

**9** Complete first ASV scan and remediation if needed.

**10** Produce a short evidence pack for audits and insurers.

Compliance only works when you see the full picture. Use this checklist to spot gaps across HIPAA, PCI, the FTC Safeguards Rule, the Cures Act, and the standards that vendors and insurers increasingly expect. GoCorpTech can audit your current posture, implement the right controls, and continuously monitor them so your team can stay focused on patients.

Schedule a compliance readiness audit with GoCorpTech to identify gaps and protect your practice.