HIPAA Agent

by Sentinel Health Compliance

HIPAA Compliance Assessment

External Risk Posture Report

Sacramento Family Dental

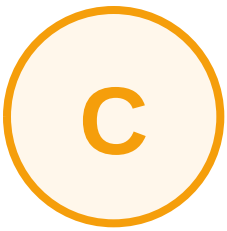
NPI: 1234567890

Sacramento, CA

www.sacramentofamilydental.com

Assessment Date: February 28, 2026

HIPAA Agent Compliance Score™



C (68/100)

Moderate Compliance Posture

8 findings identified across 4 compliance domains

2	3	3	0
Critical	High	Medium	Low

Table of Contents

Section 1: Executive Summary

HIPAA Agent conducted a comprehensive external compliance assessment of Sacramento Family Dental to evaluate the practice's externally observable compliance posture across multiple domains including email authentication, web application protection, encryption standards, network exposure, and regulatory compliance.

Key Findings

• 2 CRITICAL findings requiring immediate attention (DMARC missing, RDP exposed)
• 3 HIGH severity findings affecting email integrity and web security
• 3 MEDIUM severity findings related to encryption and compliance gaps

The practice received an HIPAA Agent Compliance Score™ of C (68/100), indicating a Moderate Compliance Posture. Immediate remediation of critical findings is recommended to reduce exposure to OCR enforcement actions and protect patient health information (PHI).

Section 2: Practice Information

Practice Name	Sacramento Family Dental
NPI	1234567890
Provider Type	Individual (NPI-1)
Specialty	General Dentistry
Address	4521 Arden Way, Sacramento, CA 95864
Website	www.sacramentofamilydental.com
HIPAA Agent Compliance Score™	C (68/100)
Compliance Posture	Moderate Compliance Posture
Assessment Date	February 28, 2026
Assessment Type	External Compliance Assessment

Section 3: Compliance Assessment Results

HIPAA Agent Compliance Score™: C (68/100)

Category Breakdown:

Email Security	2 findings	F
Web Security	3 findings	D
Network Security	1 finding	F
Encryption	1 finding	C
Compliance	1 finding	D

Section 4: HIPAA Regulatory Analysis

The following HIPAA Security Rule sections are implicated by the findings in this assessment:

§164.308(a)(5)(ii)(B)

Security Awareness and Training

Email domain spoofing vulnerability enables phishing attacks targeting staff and patients.

§164.312(e)(1)

Transmission Security

Missing DKIM authentication and weak cipher suites compromise data-in-transit integrity.

§164.312(e)(2)(ii)

Encryption

HSTS not enforced, weak ciphers accepted — encrypted channel can be downgraded.

§164.312(d)

Person or Entity Authentication

Administrative login page exposed without additional access controls.

§164.312(a)(1)

Access Control

RDP service exposed to public internet — primary ransomware attack vector.

§164.520

Notice of Privacy Practices

No privacy policy detected on practice website.

Section 5: Risk Classification & OCR Enforcement Context

Based on the findings in this assessment, the practice's maximum fine exposure under the HIPAA Enforcement Rule is estimated below. These represent potential penalties if OCR were to investigate and find willful neglect of these compliance requirements.

Penalty Tier	Per Violation	Annual Max
Tier 1 — Did Not Know	$100–$50,000	$25,000/yr
Tier 2 — Reasonable Cause	$1,000–$50,000	$100,000/yr
Tier 3 — Willful Neglect (Corrected)	$10,000–$50,000	$250,000/yr
Tier 4 — Willful Neglect (Not Corrected)	$50,000–$1,500,000	$1,500,000/yr

With 2 CRITICAL and 3 HIGH findings, this practice falls in an elevated risk category. The exposed RDP port alone is the #1 attack vector for healthcare ransomware and would likely be classified as willful neglect if not remediated.

Section 6: Detailed Findings & Violations

1. DMARC Record Not Configured

CRITICAL

Category: Email Security

No DMARC DNS record found. The practice domain can be spoofed in phishing emails targeting patients and staff, leading to potential PHI disclosure.

HIPAA Reference: §164.308(a)(5)(ii)(B) - Security Awareness and Training

Remediation: Add a DMARC record: _dmarc.example.com TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@example.com"

Fine Exposure: $50,000–$1,500,000 per violation

2. DKIM Email Signing Not Configured

HIGH

Category: Email Security

No DKIM signatures detected. Email recipients cannot verify messages actually originated from the practice domain.

HIPAA Reference: §164.312(e)(1) - Transmission Security

Remediation: Configure DKIM signing through your email provider (Google Workspace, Microsoft 365, etc.)

Fine Exposure: $10,000–$50,000 per violation

3. HTTP Strict Transport Security Not Enabled

HIGH

Category: Web Security

The website does not enforce HSTS, allowing potential SSL stripping attacks that could intercept patient form submissions.

HIPAA Reference: §164.312(e)(2)(ii) - Encryption

Remediation: Add header: Strict-Transport-Security: max-age=31536000; includeSubDomains

Fine Exposure: $10,000–$50,000 per violation

4. Administrative Login Page Publicly Accessible

HIGH

Category: Web Security

The /wp-admin login page is publicly accessible, providing an attack surface for brute-force credential attacks.

HIPAA Reference: §164.312(d) - Person or Entity Authentication

Remediation: Restrict admin access by IP, add two-factor authentication, or use a non-standard login URL.

Fine Exposure: $10,000–$50,000 per violation

5. No Privacy Policy Detected

MEDIUM

Category: Compliance

No privacy policy page was found on the practice website. HIPAA requires covered entities to provide a Notice of Privacy Practices.

HIPAA Reference: §164.520 - Notice of Privacy Practices

Remediation: Publish a HIPAA-compliant Notice of Privacy Practices on the website with a clear link in the footer.

Fine Exposure: $100–$50,000 per violation

6. Weak TLS Cipher Suites Accepted

MEDIUM

Category: Encryption

The web server accepts weak cipher suites (TLS_RSA_WITH_AES_128_CBC_SHA) that are vulnerable to known attacks.

HIPAA Reference: §164.312(e)(2)(ii) - Encryption

Remediation: Disable CBC-mode and RSA key exchange ciphers. Enable only AEAD cipher suites (AES-GCM, ChaCha20-Poly1305).

Fine Exposure: $100–$50,000 per violation

7. Content Security Policy Header Missing

MEDIUM

Category: Web Security

No Content-Security-Policy header detected, increasing risk of cross-site scripting (XSS) attacks on patient-facing pages.

HIPAA Reference: §164.312(c)(1) - Integrity Controls

Remediation: Implement a Content-Security-Policy header restricting script sources to trusted origins.

Fine Exposure: $100–$50,000 per violation

8. Remote Desktop Protocol (RDP) Exposed

CRITICAL

Category: Network Security

Port 3389 (RDP) is open and accessible from the internet. RDP is the #1 attack vector for ransomware targeting healthcare.

HIPAA Reference: §164.312(a)(1) - Access Control

Remediation: Block port 3389 at the firewall. Use VPN for remote access. Enable Network Level Authentication if RDP must remain.

Fine Exposure: $50,000–$1,500,000 per violation

Section 7: Recommendations & Remediation Steps

Based on the findings in this compliance assessment, the following remediation steps are recommended in order of priority:

IMMEDIATE **Block RDP Access**

Close port 3389 at the firewall. Implement VPN for any remote access needs. This is the single highest-risk finding.

IMMEDIATE **Implement DMARC**

Add a DMARC record with p=quarantine policy. This prevents domain spoofing and protects patients from phishing.

HIGH **Configure DKIM**

Enable DKIM signing through your email provider to authenticate all outgoing messages.

HIGH **Enable HSTS**

Add the Strict-Transport-Security header to enforce HTTPS connections and prevent SSL stripping.

HIGH **Secure Admin Login**

Restrict /wp-admin access by IP or add 2FA. Consider changing the login URL.

MEDIUM **Publish Privacy Policy**

Create and publish a HIPAA-compliant Notice of Privacy Practices on the website.

MEDIUM **Upgrade TLS Ciphers**

Disable weak CBC-mode ciphers. Only allow AEAD cipher suites.

MEDIUM **Add CSP Header**

Implement Content-Security-Policy to prevent cross-site scripting attacks.

ONGOING **Schedule Periodic Compliance Assessments**

Continuous monitoring detects new risks and tracks remediation progress over time.

Section 8: Assessment Methodology

This compliance assessment evaluates the externally observable compliance posture of the practice using HIPAA Agent's proprietary comprehensive assessment methodology. Data is collected from publicly available sources including DNS records, SSL/TLS certificates, HTTP responses, network services, web application content, breach databases, and domain intelligence to build a complete picture of the practice's external risk posture.

Assessment Scope:

- Email Authentication: SPF, DKIM, DMARC, MX record analysis
- Web Security: SSL/TLS configuration, security headers, CMS detection, exposed paths
- Network Exposure: Port scanning across all resolved IPs (bare domain + www)
- Encryption: TLS version support, cipher suite analysis, certificate chain validation
- Compliance: Privacy policy detection, cookie consent, HIPAA regulatory mapping
- Breach Intelligence: Cross-reference against HHS breach portal and dark web databases

HIPAA Agent Compliance Score™ Grading:

A (90-100): Excellent compliance posture. Minimal findings, strong controls.

B (80-89): Good compliance posture. Minor improvements recommended.

C (68-79): Moderate compliance posture. Several findings requiring attention.

D (50-67): Poor compliance posture. Significant gaps in HIPAA compliance.

F (0-49): Failing compliance posture. Critical vulnerabilities requiring immediate action.

Section 9: About HIPAA Agent

HIPAA Agent is an AI-powered HIPAA compliance agent designed specifically for healthcare practices. Your agent delivers:

- HIPAA Monitor ($99/month): Comprehensive external HIPAA compliance assessment with monthly monitoring, score tracking, email alerts, and downloadable PDF reports. hipaaagent.ai/pricing
- Free Lookup Portal: Enter your NPI at hipaaagent.ai/lookup to view your compliance assessment results instantly — no signup, no credit card.
- Breach Report Database: Real-time tracking of HHS-reported healthcare breaches with AI-generated analysis. hipaaagent.ai/breach-report
- Policy Documents: 18 customizable HIPAA policy templates for covered entities. hipaaagent.ai/policies
- Staff Training: 6 interactive HIPAA training modules with completion certificates. hipaaagent.ai/training

For questions about this assessment, contact compliance@hipaaagent.ai