April 2026 Technical Risk Assessment

Blue Trust Dental Associates · Austin, TX

DIGITAL PRESENCE SECURITY SCORE

850

out of 1000

B

PERIOD	April 2026
SCANS THIS PERIOD	4
CHANGE VS PRIOR MONTH	+32 pts
PEER MEDIAN (DENTAL — GENERAL, US)	782

FINDINGS SUMMARY

PERIOD	April 2026
SCANS THIS PERIOD	4
OPEN FINDINGS	7
RESOLVED THIS PERIOD	2
BY SEVERITY	1 critical · 2 high · 3 medium · 1 low

Non-BA service. Blue Trust is not a HIPAA Business Associate. This report is generated from scans of public-facing surfaces only; Blue Trust does not access, store, or process protected health information.

Generated Fri, 01 May 2026 08:30:00 GMT · Template dpra-v1 · Scoring v1.4.2

Findings

CRITICAL `45 CFR §164.502(a); OCR Tracking Bulletin (Mar 2024)`

Meta (Facebook) Pixel detected on patient-facing pages

A Meta Pixel (id 845207193001782) is loaded on the homepage and the Schedule Appointment page. It transmits page views and button clicks — including the user agent and the page URL with any query parameters — to Facebook. Meta is generally not a HIPAA Business Associate for healthcare practices.

Location: `https://bluetrustdental.example/schedule`

> **Remediation:** Remove the Meta Pixel from any page that lists clinical services, schedules, or accepts patient input. If marketing requires a pixel, gate it through a server-side conversion API and a documented BAA — Meta will not sign one. Class actions over Meta Pixel on healthcare sites have settled for $6.6M (Novant Health, 2024) and $12.25M (Advocate Aurora, 2022).

HIGH `45 CFR §164.504(e); HIPAA BAA requirement`

New-patient intake form posts to a vendor without a BAA

The form at /new-patient submits via JotForm. JotForm is HIPAA-eligible only on its enterprise tier with a signed BAA in place. The current form is using the free tier (verified by the absence of the HIPAA badge in the form footer).

Location: `https://bluetrustdental.example/new-patient`

> **Remediation:** Migrate the form to JotForm HIPAA (or to your dental software's native intake) and execute a BAA before publishing the new endpoint. Until then, replace the form with a phone-and-email contact block.

HIGH `NIST SP 800-177 §4.5; Google + Yahoo bulk-sender requirements (Feb 2024)`

DMARC policy permits domain spoofing (p=none)

The DMARC record published at _dmarc.bluetrustdental.example is set to p=none, which instructs receiving mail servers to take no action on messages that fail authentication. An attacker can send messages that appear to come from the practice — e.g. a fake billing or patient-confirmation email — and they will land in the inbox.

> **Remediation:** Stage to p=quarantine after one full reporting cycle, then to p=reject. Add an rua= reporting address so failures are visible. Most managed mail providers (Google Workspace, Microsoft 365) ship a one-click DMARC quarantine flow.

MEDIUM `OWASP ASVS §14.4; HHS HICP 2023 §3.2`

Content Security Policy header missing

The homepage response does not include a Content-Security-Policy header. A CSP is the single most effective protection against script injection on a website that loads third-party tools. Without it, a compromise of an upstream vendor (analytics, scheduling widget, chat tool) can quietly inject script that runs on every patient-facing page.

Location: `https://bluetrustdental.example/`

> **Remediation:** Issue a starting CSP in report-only mode for two weeks, review the violation reports, then enforce. Recommended starting policy: default-src 'self'; script-src 'self' https://www.googletagmanager.com; img-src 'self' data:; frame-ancestors 'none'.

MEDIUM `RFC 6797; HHS HICP 2023 §3.2`

HSTS header missing

The site responds over HTTPS but does not advertise HTTP Strict Transport Security. A first-time visitor on an untrusted network can be downgraded to HTTP via SSL stripping before they ever reach an HTTPS page.

Location: `https://bluetrustdental.example/`

> **Remediation:** Add Strict-Transport-Security: max-age=31536000; includeSubDomains. After 30 days of stable HTTPS-only operation, add ; preload and submit the domain to hstspreload.org.

MEDIUM `FTC HBNR §318.6; OCR Tracking Bulletin (Mar 2024)`

Privacy policy last updated more than 24 months ago

The privacy policy at /privacy is dated 2023-09-12. It does not reflect the FTC Health Breach Notification Rule changes effective July 2024, the OCR tracking-bulletin clarifications from March 2024, or the practice's current vendor list (Calendly was added Q4 2024 but is not disclosed).

Location: `https://bluetrustdental.example/privacy`

> **Remediation:** Refresh the policy quarterly using the Blue Trust template. Disclose every third-party that receives any personal information, even when behind a BAA. Add a versioned change log at the bottom.

LOW `NIST SP 800-52r2`

TLS 1.0/1.1 still negotiable on port 443

The site negotiates TLS 1.0 and TLS 1.1 in addition to TLS 1.2 / 1.3. Both deprecated versions are now rejected by every supported browser; remaining clients are typically scanners and bots.

Location: `https://bluetrustdental.example/`

> **Remediation:** Disable TLS 1.0 and 1.1 at the host or CDN. On Cloudflare: SSL/TLS → Edge Certificates → Minimum TLS Version → 1.2.

Patient Reviews

Daily monitoring across Google Business, Yelp, Healthgrades, and Zocdoc. Each new review is run through an automated classifier that flags language that could trigger a HIPAA Privacy Rule violation if responded to publicly (45 CFR §164.502). Vitals + RateMDs expanding 2026 Q3.

314
TOTAL REVIEWS TRACKED

4.6
AVERAGE RATING

4
PRIVACY-SENSITIVE FLAGS

By platform

PLATFORM	REVIEWS	AVERAGE RATING
Google Business	182	4.7
Yelp	64	4.3
Healthgrades	47	4.8
Zocdoc	21	4.5

Privacy-sensitive reviews this period

1. Google Business · 2★ · 2026-04-12
   "They gave me the wrong dosage of lidocaine and I had to go to urgent care. Still waiting for someone to call me back about the prescription mix-up."

2. Yelp · 5★ · 2026-04-08
   "Dr. M. was wonderful with my 6 year old daughter Sarah. She has special needs and they were patient with her cleaning and the cavity filling. We will definitely come back."

3. Healthgrades · 1★ · 2026-04-22
   "I have been a patient here for 7 years. After my last crown they billed my insurance twice and refused to refund the difference. I am filing a complaint with the state board."

4. Google Business · 4★ · 2026-04-27
   "Came in for an Invisalign consultation as a referral from Dr. Roberts. The treatment plan they laid out was reasonable. The only issue was the wait time."

Reputation Management

Weekly enumeration of typosquat / lookalike domains, dangling subdomains vulnerable to takeover, and credential-breach exposure for staff emails (sourced from the Have I Been Pwned breach corpus). Findings here are not on your website itself — they're about adversary infrastructure or previously-leaked credentials that affect your practice.

3
REGISTERED TYPOSQUATS

1
SUBDOMAIN TAKEOVER RISKS

2
BREACHED-CREDENTIAL MATCHES

Active findings

TYPE	TARGET	SEVERITY	FIRST SEEN
Typosquat domain	bluetrustdental-tx.example	MEDIUM	2026-04-02
	Registered 2025-11-04 via Namecheap; resolves to a parking page.		
Typosquat domain	bluetru5tdental.example	MEDIUM	2026-04-02
	Homoglyph substitution (s → 5). Registered 2026-02-19, parking page, no MX records.		
Subdomain takeover risk	old.bluetrustdental.example	CRITICAL	2026-04-10
	CNAME points at an unclaimed AWS S3 bucket. Body returned "NoSuchBucket" — an attacker can register the bucket and serve content as your subdomain.		
Credential-breach exposure	dr.smith@bluetrustdental.example (LinkedIn 2023)	HIGH	2026-03-15
	Appeared in the 2023 LinkedIn breach (704M records). Sensitive data class: passwords, geographic locations.		
Credential-breach exposure	frontdesk@bluetrustdental.example (Dropbox 2022)	MEDIUM	2026-03-15
	Appeared in the 2022 Dropbox internal repository leak. No password hashes exposed; email addresses + names only.		

Regulatory Intelligence

New regulatory enforcement events and federal class-action filings, filtered to your specialty and region. Sources: HHS Office for Civil Rights Wall of Shame (refreshed daily), CourtListener federal court filings (refreshed daily). State Attorney General digest expanding 2026 Q3.

OCR WALL OF SHAME · MA · 2026-04-19

Massachusetts Dental Group: 47,200 affected

Unauthorized access / disclosure. Network server. Type: hacking/IT incident.

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

FEDERAL CLASS ACTION · D. MASS. · 2026-04-15

Doe v. Northgate Dental Associates — Meta Pixel class action (D. Mass.)

Federal class action alleging Meta Pixel on appointment booking page disclosed PHI without authorization. Filed under 18 U.S.C. § 2511 and HIPAA.

Source: https://www.courtlistener.com/

OCR WALL OF SHAME · TX · 2026-04-08

Texas Pediatric Dentistry, P.A.: 8,400 affected

Improper disposal of paper/films. Type: improper disposal.

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

FEDERAL CLASS ACTION · S.D. TEX. · 2026-04-02

Patel v. Lone Star Family Dental — session replay class action (S.D. Tex.)

CIPA / federal wiretap claims over Microsoft Clarity session replay capturing patient-form keystrokes. Settled in principle (terms sealed).

Source: https://www.courtlistener.com/

OCR WALL OF SHAME · FL · 2026-03-28

Florida Orthodontic Group: 12,600 affected

Hacking/IT incident. Email phishing → credential reuse → patient record access.

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Methodology

This report is produced from automated scans of public-facing digital surfaces on behalf of **Blue Trust Dental Associates**. The monitoring is designed to satisfy the documentation requirement of 45 CFR §164.308(a)(1)(ii)(A) — a defensible evidence trail that the practice conducted an ongoing review of its digital risk posture.

Surfaces monitored

- Website security
- Email authentication
- Privacy compliance
- Patient reviews
- Brand & reputation

What we scanned

DNS & email authentication (DMARC, SPF, DKIM, CAA), HTTP security headers (HSTS, CSP, X-Frame-Options), SSL/TLS configuration and certificate transparency, exposed configuration files, WordPress/CMS-level vulnerabilities, tracking pixel inventory (Meta, Google Analytics, TikTok, LinkedIn, Snap, Pinterest, session replay tools), cookie consent, privacy policy presence + freshness, CCPA opt-out, HIPAA Notice of Privacy Practices, form destinations, scheduling-widget vendors, and vertical-specific HIPAA risks including no-BAA vendor integrations and PHI in URL parameters.

Scan window

CADENCE	Daily
CHECKS RUN PER SCAN	524
EARLIEST SCAN IN PERIOD	2026-04-01T07:14:00Z
LATEST SCAN IN PERIOD	2026-04-30T23:11:00Z
SCORING ALGORITHM VERSION	v1.4.2

What this report is not

This report is not a legal opinion and does not constitute a Security Risk Analysis under HIPAA §164.308(a)(1)(ii)(A) on its own. It is a defensible evidence artifact that supplements your Security Risk Analysis workflow. The practice remains solely responsible for the breach-risk determination on any incident and for the final adoption of any policy or notice generated by the platform.

Blue Trust operates as an external digital-presence monitoring service. Blue Trust is not a Business Associate under 45 CFR §160.103 and does not receive, maintain, or transmit PHI.