Client	**Sample Dental Practice, PLLC (EXAMPLE)**
Target asset	**sampledental.com**
Assessment	Standard external assessment
Date	July 08, 2026
Prepared by	CyberShield Austin, Austin, TX

> SAMPLE REPORT — a fictitious example for illustration only. The client, target, and findings shown are not real.

Executive Summary

This report summarizes an external, non-intrusive security assessment of **sampledental.com** performed for Sample Dental Practice, PLLC (EXAMPLE) on July 08, 2026. It identifies internet-facing exposure and prioritizes remediation by business impact.

Critical exposure - immediate action required

Critical **1**
High **3**
Medium **2**
Low **3**
Info **0**

What matters most

1. **Patient database is reachable from the public internet (port 3306)** CRITICAL
   Your MySQL database is directly reachable from anywhere on the internet. A database holding patient records should never be exposed this way.
2. **No DMARC record — your domain can be spoofed** HIGH
   Without DMARC, anyone can send email that appears to come from sampledental.com. This is a common vector for invoice fraud and patient-facing phishing.
3. **2 lookalike domain(s) registered and able to send email** HIGH
   Domains that closely resemble yours are registered and have mail servers configured — commonly used to impersonate your practice to patients and staff.

Detailed Findings

Domain 1 - Attack Surface and Exposed Services

CRITICAL **Patient database is reachable from the public internet (port 3306)**

`sampledental.com:3306`

Your MySQL database is directly reachable from anywhere on the internet. A database holding patient records should never be exposed this way.

> This client handles protected health information (HIPAA) and operates a patient portal, so this exposure carries higher business impact.

```
3306/tcp open  mysql  MySQL 5.7.38
```

> **Remediation:** Firewall the database off the public internet; allow access only from the application server or over a VPN.

Domain 2 - TLS / SSL Configuration

MEDIUM TLS certificate expires in 9 day(s)

`sampledental.com:443`

The website's certificate is close to expiry. An expired certificate breaks HTTPS for every visitor with a browser security warning.

```
notAfter=Jul 17 12:00:00 2026 GMT
```

> **Remediation:** Renew the certificate now and enable automatic renewal (e.g. via Let's Encrypt / your host) so it can't lapse.

Domain 3 - Web Application Security

HIGH Missing security header: HSTS (forces browsers to use HTTPS)

`https://sampledental.com`

Without HSTS, a patient on public Wi-Fi can be silently downgraded to insecure HTTP and have portal traffic intercepted.

> Severity raised from medium to high: this client handles protected health information (HIPAA) and operates a portal application, so this exposure carries higher business impact.

> **Remediation:** Add 'Strict-Transport-Security: max-age=31536000; includeSubDomains' at the web server.

Domain 4 - Email Authentication & Domain Impersonation

HIGH No DMARC record — your domain can be spoofed

`sampledental.com`

Without DMARC, anyone can send email that appears to come from sampledental.com. This is a common vector for invoice fraud and patient-facing phishing.

> **Remediation:** Publish a DMARC record at _dmarc.sampledental.com starting at p=none to monitor, then escalate to p=quarantine and p=reject.

HIGH 2 lookalike domain(s) registered and able to send email

`sampledental.com`

Domains that closely resemble yours are registered and have mail servers configured — commonly used to impersonate your practice to patients and staff.

```
sample-dental.com
sampledentai.com
```

> **Remediation:** Review each domain; consider defensively registering the closest matches and report clear impersonators. Enforcing DMARC reduces their value to attackers.

LOW SPF record present but not enforcing (soft fail)

sampledental.com

The SPF record does not end in '-all', so spoofed mail may still be accepted by some receivers.

```
"v=spf1 include:_spf.mail.hostinger.com ~all"
```

> **Remediation:** Tighten the SPF record to end in '-all' once all legitimate senders are confirmed.

LOW No DKIM record found for common selectors

sampledental.com

DKIM signs outgoing mail so recipients can verify it wasn't forged. None was found.

> **Remediation:** Enable DKIM signing with your mail provider and publish the provided public key.

LOW MTA-STS is not configured

sampledental.com

MTA-STS protects inbound mail from downgrade attacks. It is not published.

> **Remediation:** Publish an MTA-STS policy to enforce TLS on inbound mail.

Domain 5 - DNS and Domain Hygiene

MEDIUM Potentially sensitive subdomains are publicly discoverable

sampledental.com

Subdomain names suggest non-production systems that may not be intended for public exposure.

```
dev.sampledental.com
old.sampledental.com
```

> **Remediation:** Review each host; take forgotten dev/old systems offline or behind VPN, and remove stale DNS records.

Prioritized Remediation Plan

PRIORITY	FINDING	ACTION
CRITICAL	Patient database is reachable from the public internet (port 3306)	Firewall the database off the public internet; allow access only from the application server or over a VPN.
MEDIUM	TLS certificate expires in 9 day(s)	Renew the certificate now and enable automatic renewal (e.g. via Let's Encrypt / your host) so it can't lapse.
HIGH	Missing security header: HSTS (forces browsers to use HTTPS)	Add 'Strict-Transport-Security: max-age=31536000; includeSubDomains' at the web server.
HIGH		

PRIORITY	FINDING	ACTION
	No DMARC record — your domain can be spoofed	Publish a DMARC record at _dmarc.sampledental.com starting at p=none to monitor, then escalate to p=quarantine and p=reject.
HIGH	2 lookalike domain(s) registered and able to send email	Review each domain; consider defensively registering the closest matches and report clear impersonators. Enforcing DMARC reduces their value to attackers.
LOW	SPF record present but not enforcing (soft fail)	Tighten the SPF record to end in '-all' once all legitimate senders are confirmed.
LOW	No DKIM record found for common selectors	Enable DKIM signing with your mail provider and publish the provided public key.
LOW	MTA-STS is not configured	Publish an MTA-STS policy to enforce TLS on inbound mail.
MEDIUM	Potentially sensitive subdomains are publicly discoverable	Review each host; take forgotten dev/old systems offline or behind VPN, and remove stale DNS records.

Methodology and Scope

The assessment followed CyberShield Austin's six-domain external methodology: attack surface, TLS/SSL, web security, email authentication, DNS hygiene, and public exposure. Testing was **external and non-intrusive** and performed under signed authorization.

Out of scope: exploitation, password brute-forcing, denial-of-service, and any asset not named on the authorization form.

Controls verified as present

- CSP (blocks injected/malicious scripts) is set
- X-Frame-Options (clickjacking protection) is set
- X-Content-Type-Options (blocks MIME sniffing) is set
- No weak TLS protocols or known TLS vulnerabilities detected
- DNS zone transfer (AXFR) is not allowed

This assessment was performed externally and non-intrusively under signed authorization. It reflects the target's exposure at the time of testing.

CyberShield Austin · cybershieldaustin.com · info@cybershieldaustin.com