WEBSITE RISK & EXPOSURE REPORT

A medical practice

Overall risk: Moderate

REPORT DATE	PAGES REVIEWED	INDUSTRY PROFILE	SCAN MODE
August 19, 2026	4	Medical practice	read-only

Document control

Subject site	**A medical practice**	Report reference	**—**
Scan date	**August 19, 2026**	Report version	**Full**
Scan mode	**read-only**	Coverage	**complete**
Pages scanned	**4**	Engine version	**v0.2.0**
Industry profile	**Medical practice**	Overall verdict	**Moderate**

Scope of this report

This is a point-in-time automated technical scan of observable website behavior on the specific URLs scanned, as they existed at the scan date shown — not a legal compliance audit or attestation, and not an audit, certification, or compliance opinion of any kind. Results describe only the pages scanned at that time; they are not an assessment of the business or entity operating the site, and must not be represented as current after the scan date. A "pass" means no high-priority technical issues were found at the scan threshold on the pages crawled — it does not certify HIPAA, ADA, or any regulatory compliance, and does not cover items unobservable from outside (signed vendor agreements, server configuration, internal policies). Form analysis covers each form's declared submission target; forms that submit via JavaScript to endpoints not visible in the page markup are not assessed. Third-party/tracker detection matches a known-vendor catalog, so absence of a finding is not proof a site is free of trackers. This report is general information about observable technical facts and is not legal advice, does not create an attorney-client or other professional relationship, and is not a substitute for review by a qualified attorney. For your specific legal obligations, consult an attorney licensed in your jurisdiction. The exact URLs scanned are enumerated in the appendix at the end of this report.

Contents

1 Executive Summary

ACTION REQUIRED **4 high-priority technical issue(s) found in this scan**

This assessment identified **4 high-severity** issues that should be addressed. The most significant exposure is concentrated in accessibility (ada) and regulated-data privacy.

> **Why this verdict:** The verdict is Moderate, driven by 1 high-severity finding in the risk areas the verdict covers (compliance, privacy and security).

DO THESE FIRST

- **HIGH** **Navigation & links** — Included in accessible-names fix
- **HIGH** **Form accessibility** — Give every control, link and field an accessible name
- **HIGH** **Site platform & vendors** — Replace built-in platform forms with a covered vendor

0	4	6	18	28
CRITICAL	HIGH	MEDIUM	LOW	TOTAL

SEO	PERFORMANCE	UX
58/100	96/100	22/100

Technical scores: 100 less a fixed deduction per issue found — they rank your own scans against each other, not your site against anyone else's. Compliance, privacy and security risk are reported as a verdict, never a number.

HOW THESE SCORES WERE CALCULATED

SEO · 58/100

100 start
−10 1 page(s) have very little text content · Medium
−4 75% of pages lack a meta description · Low
−4 Images missing alt text on 1 page(s) · Low
−4 Heading levels skip on 4 page(s) · Low
−4 1 page(s) have a missing or duplicated main heading (H1) · Low
−4 1 page title(s) are too short or too long for search results · Low
−4 Business structured data is missing key fields · Low
−4 1 meta description(s) are outside the ideal length · Low

−4 No tap-to-call phone link detected · Low

↳ resolving "1 page(s) have very little text content" alone → **68/100**

Performance · 96/100
100 start
−4 32 image(s) have no width/height attributes · Low

↳ resolving "32 image(s) have no width/height attributes" alone → **100/100**

UX · 22/100
100 start
−20 Links with no accessible name on 4 page(s) · High
−20 Form fields without labels on 1 page(s) — unusable with a screen reader · High
−20 Buttons with no accessible name on 4 page(s) · High
−10 Images missing alt text on 1 page(s) · Medium
−4 Heading levels skip on 4 page(s) · Low
−4 No accessibility statement page · Low

↳ resolving "Links with no accessible name on 4 page(s)" alone → **42/100**

HOW TO READ THIS REPORT

Severity ranks how much attention an item warrants: **Critical** rests on an observed fact on a sensitive page; **High** is a strong exposure; Medium/Low are lower-priority. **Observed vs. verify**: we report what we saw leave the browser as fact; anything we cannot see from outside (a signed agreement, a server config) we mark to verify, never assert. "Sensitive context" means a page whose URL, title, or form indicates health, identity, or payment data.

What to do, in order

16 changes, in the order we would make them — 18 of the 28 items are covered by just 6 of them, because one change can settle several at once.

1 **Give every control, link and field an accessible name** clears 3 items HIGH

Accessibility (ADA) · Form accessibility / Navigation & links

Add the missing programmatic name to each control we list — a visible <label for=…>, an aria-label on icon-only buttons and links, a <title> on frames, and a text alternative on meaningful SVG. We name the exact elements.

We can supply the exact change to apply.

2 **Replace built-in platform forms with a covered vendor** HIGH

Regulated-Data Privacy · Site platform & vendors

Swap the site builder's native forms for an embedded form from a vendor that signs your data agreement; export and purge stored submissions. The site itself stays put.

We can arrange this with a specialist.

3 Security headers clears 5 items MEDIUM

Website Security · Security headers

Resolved by the security-headers change.

We can supply the exact change to apply.

Add these response headers

Your Wix response-header settings, or the CDN in front of it if one is serving these pages.

SEND ON EVERY HTML RESPONSE

```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Content-Security-Policy-Report-Only: default-src 'self'; frame-ancestors 'none'; object-src 'none'; base-uri 'self'
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
Permissions-Policy: geolocation=(), camera=(), microphone=(), payment=()
```

- An HSTS header is already present but short-lived or scoped to one host; the value above is the long-lived, subdomain-wide form.
- Only send HSTS once every subdomain is reachable over https — it is not reversible for the max-age you publish.
- CSP is the one header that can break a working page, so it is given in REPORT-ONLY form. Run it, read the violation reports, widen it for the third parties you actually use, then rename the header to Content-Security-Policy.

4 Add image alt text clears 2 items MEDIUM

Accessibility (ADA) + SEO & Findability · Page content / Screen-reader structure

Descriptive alt text on meaningful images; empty alt on decorative ones.

We can supply the exact change to apply.

Add image alt text

The templates or components that render these images.

WHAT EACH NEEDS

```
<img src="team.jpg" alt="Dr Chen with a patient in the consulting room">
<img src="divider.png" alt="">
```

- Describe what the image CONVEYS in context, not what it contains. A decorative image takes alt="" — an empty alt is correct and is not the same as a missing one.
- Alt text is the one item here we cannot generate: only you know what each image is meant to say.

5 Set up SPF & DMARC email authentication clears 2 items MEDIUM

Website Security · Email security

Publish SPF and DMARC DNS records so forged email from your domain gets rejected and real mail lands in inboxes.

We can supply the exact change to apply.

Publish these DNS records

Your DNS host for example-practice.com (wherever the nameservers point).

DNS RECORDS

```
example-practice.com    TXT     v=spf1 include:_spf.google.com -all
_dmarc.example-practice.com     TXT     v=DMARC1; p=reject; rua=mailto:contact@example.com
```

- Your current SPF ends in a soft fail, so forgeries are delivered anyway. Above is your existing record with the ending changed to -all. Confirm every service that sends mail as you is listed before switching.
- A DMARC record exists but is in monitor-only mode, so nothing is actually rejected. Move to p=quarantine first and read the reports before p=reject.

6 Expand thin service pages MEDIUM

SEO & Findability · Page content

Rewrite key service pages to 300+ words around real patient questions.

We can arrange this with a specialist.

7 Set secure flags on session cookies MEDIUM

Website Security · Security headers

HttpOnly, Secure, and SameSite on session/auth cookies.

We can supply the exact change to apply.

Set the missing cookie attributes

Wherever these cookies are issued — your application's session settings, or the platform setting that controls them.

THE ATTRIBUTES EACH SESSION/AUTH COOKIE NEEDS

```
Set-Cookie: <name>=<value>; Secure; HttpOnly; SameSite=Lax; Path=/
```

- Secure stops the cookie travelling over plain http; HttpOnly stops scripts reading it; SameSite=Lax stops it riding along on cross-site requests.
- Use SameSite=None only where a cookie genuinely must cross sites — and it then also requires Secure.

8 Fix page headings clears 3 items LOW

Accessibility (ADA) + SEO & Findability · Page content / Screen-reader structure

One clear H1 per page; demote extras.

We can supply the exact change to apply.

Fix the heading structure

The page templates — heading level is structure, not size.

THE HEADING OUTLINE WE OBSERVED

```
/   h1 → h3 → h2 → h3 → h2 → h6 → h6 → h6 → h6 → h6 → h6 → h6 → h3 → h2 → h6 → h6 → h6
/services   h3 → h1 → h3 → h3 → h3 → h3 → h3 → h3 → h3 → h2 → h2
/contact   h3 → h1 → h1 → h3 → h3 → h3 → h3
/service-page/1-testosterone-hormone-consultation   h1 → h2 → h3 → h2 → h5 → h5 → h5 → h5 → h5 → h5 → h2
```

WHAT A CORRECT OUTLINE LOOKS LIKE

```
<h1>One per page — what this page is about</h1>
  <h2>A section</h2>
    <h3>A subsection</h3>
  <h2>The next section</h2>
```

- Exactly one h1 per page, and never skip a level on the way down — a screen-reader user navigates by these, and a jump from h2 to h4 reads as a missing section.
- If a heading is the wrong SIZE, change the CSS. Changing the level to get a font size is what produces these outlines.

9 Titles & meta clears 3 items LOW

SEO & Findability · Search findability

Resolved by the titles & meta work.

We can supply the exact change to apply.

10 Publish an accessibility statement LOW

Accessibility (ADA) · Accessibility posture

Conformance target, known limitations, and a help contact, linked in the footer.

We can supply the exact change to apply.

11 DNS hardening LOW

Website Security · DNS & certificate control

Resolved by the DNS-hardening work.

We can supply the exact change to apply.

Publish these DNS records

Your DNS host for example-practice.com (wherever the nameservers point).

DNS RECORDS

```
example-practice.com    CAA     0 issue "YOUR-CA"
```

- Replace YOUR-CA with the certificate authority you actually use (letsencrypt.org, digicert.com, ...). A CAA record naming a CA you do not use will stop your renewals.

12 Image optimization LOW

SEO & Findability · Speed & mobile

We can supply the exact change to apply.

Give images explicit dimensions

The templates or components that render these images.

GIVE EVERY IMAGE ITS NATURAL SIZE SO THE PAGE STOPS JUMPING

```
<img src="hero.jpg" alt="…" width="1200" height="800">
```

- width/height are the intrinsic pixel size, not the display size — CSS still controls how it renders. They exist so the browser can reserve the space before the image loads.

13 Structured data LOW

SEO & Findability · Local SEO & business info

Resolved by the schema work.

We can supply the exact change to apply.

Add structured data for the business

The <head> of your homepage (and each location page, if you have more than one).

JSON-LD

```
<script type="application/ld+json">
{
  "@context": "https://schema.org",
  "@type": "LocalBusiness",
  "name": "YOUR BUSINESS NAME",
  "url": "https://example-practice.com/",
  "telephone": "9739340152",
  "address": {
    "@type": "PostalAddress",
    "streetAddress": "STREET",
    "addressLocality": "CITY",
    "addressRegion": "STATE",
    "postalCode": "ZIP"
  }
}
</script>
```

- The phone number above is the one we observed on the site. The address fields are placeholders — we can count the addresses on your pages but not read them reliably enough to publish as structured data.
- Use the @type that fits (MedicalClinic, Dentist, LegalService…) rather than the generic LocalBusiness where a specific one exists.
- We saw more than one address on this site — each location needs its own block, on its own page.

14 Add Subresource Integrity to third-party scripts LOW

Website Security · Security headers

Pin third-party scripts/styles with integrity hashes, or self-host the critical ones.

We can supply the exact change to apply.

15 Make phone number tap-to-call LOW

SEO & Findability · Conversion & trust

Convert the header number to a tel: link.

We can supply the exact change to apply.

Make the phone number tappable

Everywhere the number appears — header, footer, contact page.

WRAP THE NUMBER IN A TEL: LINK

```
<a href="tel:+15550000000">9739340152</a>
```

- The number above is the one we observed on your pages. tel: wants E.164 — country code first, digits only — while the visible text can stay formatted however you like.
- We assumed a +1 country code; change it if that is wrong.

16 TLS hardening LOW

Website Security · Transport security

We can supply the exact change to apply.

Ordered by severity, then by how many items one change settles. Cost are deliberately NOT part of that order — cheapest-first would sell you the easy work rather than the work that matters.

2 The evidence

What your site is costing you

Every observation from this scan, grouped by what it actually does to your business — the same five groups as your portal, ordered by severity. We describe how each one affects you; we never put a number on it, because that number would be a guess about your business rather than an observation about your site.

People who can't use your site

8 observations

Who arrives, hits something they cannot get past, and leaves?

3 High **1 Medium** **4 Low**

- Links with no accessible name on 4 page(s)
- Form fields without labels on 1 page(s) — unusable with a screen reader
- Buttons with no accessible name on 4 page(s)

and 5 more in this group

Details: the Accessibility · Speed & mobile · Search & findability chapters in the findings below.

The tools and tags you're running

1 observation

What is on your site, who put it there, and is it doing anything?

1 High

- Site runs on Wix; its standard plan is not offered with a Business Associate Agreement (BAA) — verify before its forms collect protected health information (PHI)

Details: the Privacy & tracking chapter in the findings below.

How exposed you are

11 observations

What does your site tell the outside world about how it is configured?

4 Medium **7 Low**

- No Content-Security-Policy — injected scripts run unrestricted
- Pages leak their full address to outside services (no Referrer-Policy)
- DMARC is in monitor-only mode (p=none) — forgeries still get delivered

and 8 more in this group

Details: the Security posture chapter in the findings below.

Being found

8 observations

Can the pages you want found actually be found, and read correctly?

1 Medium **7 Low**

- 1 page(s) have very little text content
- 75% of pages lack a meta description
- Images missing alt text on 1 page(s)

and 5 more in this group

Details: the Search & findability chapter in the findings below.

Checked, nothing found: what you're promising. A real result about the pages we crawled — not a guarantee.

What left the visitor’s browser

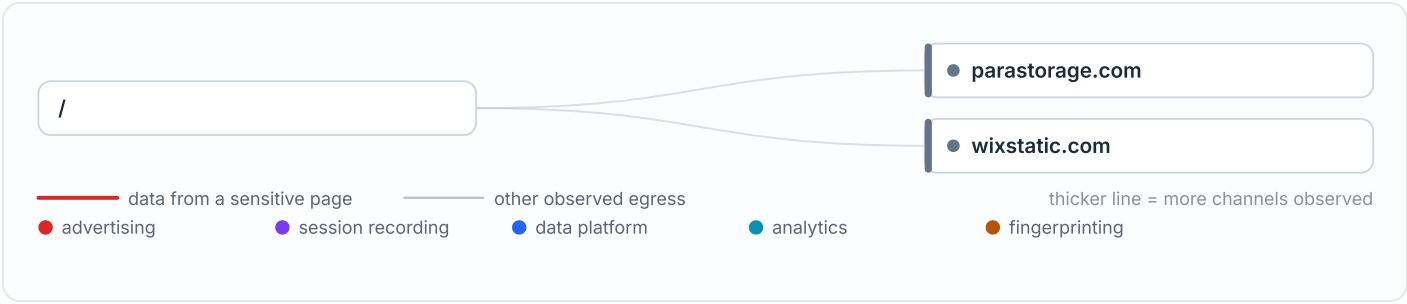
We recorded what each third party received from the pages we scanned. **2** distinct third parties received data from this site.

DESTINATION	TYPE	PAGES	HOW DATA WAS SENT
parastorage.com	Third party	1	requests pre-consent
wixstatic.com	Third party	1	requests pre-consent

Observed transmissions, captured as they happened — not inferred from a script being present. We report what left and to whom; we do not assert any recipient is unauthorized. Verify each is a disclosed, consented, and (where required) contractually covered destination.

How data flows off your site

Each line is an observed transmission from one of your pages to a third party. **Red** lines carry data from a page with sensitive context; thicker lines carried data over more channels.



Risk overview

AREA	HIGHEST	FINDINGS	SEVERITY MIX
Accessibility (ADA)	HIGH	6	3 High, 1 Medium, 2 Low
Regulated-Data Privacy	HIGH	1	1 High
Website Security	MEDIUM	11	4 Medium, 7 Low
SEO & Findability	MEDIUM	10	1 Medium, 9 Low

Findings

Findings are organised into the same six discipline chapters as your portal, then grouped by area and numbered **area.item** (3.2 = area 3, item 2). A sensitive tag marks a page whose URL, title, or form indicated health, identity, or payment context — the specific trigger is shown where recorded.

Privacy & tracking Moderate risk

What is on your site, what is leaving it, and whether you can name where it goes. **1 observation in this discipline.**

1 Site platform & vendors — 1 finding

The platforms and services your site is built on and served by.

> These are the companies that can see your site's traffic and data by design. Knowing who they are is the difference between a vendor list you can answer questions about and one you cannot.

1.1 Site runs on Wix; its standard plan is not offered with a Business Associate Agreement (BAA) — verify before its forms collect protected health information (PHI) — HIGH

REGULATED-DATA PRIVACY · SITE PLATFORM & VENDORS · 78% CONFIDENCE

If no Business Associate Agreement (BAA) covers this platform, anything a visitor types into these forms is held by an uncovered vendor, so submissions containing protected health information (PHI) would have no signed vendor agreement behind them. This is easy to miss precisely because nothing visibly "leaves" the site — which is why it's worth verifying your plan's terms.

Consumer site builders' standard plans exclude regulated health data. As of June 2026, Wix offers a BAA only on eligible plans with its HIPAA mode enabled, and Squarespace's BAA covers Acuity Scheduling only — verify the specific plan. HHS treats a vendor storing PHI without a BAA as an impermissible disclosure path.

Observed: platform Wix (header x-wix-request-id; assets from static.parastorage.com; generator "Wix.com Website Builder"); 4 data-collection form(s) on 4 page(s); vendor-terms as of June 2026

> **Recommended fix:** Verify whether your Wix plan includes a Business Associate Agreement (BAA). If not, replace the built-in forms with an embedded form from a vendor that signs one (the site can stay on Wix — only the forms move), and export/purge submissions stored in the platform.

Search & findability Low risk

Whether the pages you want found can actually be found, and read correctly. **9 observations in this discipline.**
Technical score 58/100 — ranks your own scans against each other, not a grade against other sites.

2 • Page content

4 findings

How each page describes itself to search engines and to people scanning results.

> Titles and descriptions are the advert you did not know you were writing. When pages share them, they compete with each other instead of with your competitors.

2.1 1 page(s) have very little text content — MEDIUM

SEO & FINDABILITY · PAGE CONTENT · 80%

Thin service pages rarely rank for the searches patients actually type; competitors with fuller pages win those clicks.

Observed: /contact (135w)

> **Recommended fix:** Expand each key service page to 300+ words answering the questions patients ask about that service.

2.2 Images missing alt text on 1 page(s) — LOW

SEO & FINDABILITY · PAGE CONTENT · 85%

Text alternatives are what image search reads and what a screen reader announces. Without them an image contributes to neither.

Observed: /services (7 imgs)

> **Recommended fix:** Add concise, descriptive alt text to meaningful images.

2.3 Heading levels skip on 4 page(s) — LOW

SEO & FINDABILITY · PAGE CONTENT · 80%

Heading levels are the outline of the page. When they skip, both search engines and people using a screen reader lose the structure they navigate by.

Observed: / [1>3>2>3>2>6>6>6>6>6>6>6>3>2>6>6>6], /services [3>1>3>3>3>3>3>3>3>2>2], /contact [3>1>1>3>3>3>3], /service-page/1-testosterone-hormone-consultation [1>2>3>2>5>5>5>5>5>5>2]

> **Recommended fix:** Use heading levels in order — H1 for the page title, H2 for sections, H3 for sub-sections — without skipping.

2.4 1 page(s) have a missing or duplicated main heading (H1) — LOW

SEO & FINDABILITY · PAGE CONTENT · 78%

A clear single H1 helps both search engines and visitors grasp the page topic instantly.

Observed: /contact (2)

> **Recommended fix:** Set one descriptive H1 per page; demote extras to H2/H3.

3 • Search findability

3 findings

Whether search engines can reach, read and index the pages you want found.

> A page that cannot be indexed cannot earn a visit from search, no matter how good it is. This is the technical half of search — what your site makes possible — not rankings.

3.1 75% of pages lack a meta description

LOW

SEO & FINDABILITY · SEARCH FINDABILITY · 88%

A compelling description is your ad copy in search results; missing ones lower click-through even when you rank.

Observed: /, /services, /contact

> **Recommended fix:** Add a 140–160 character description per page summarizing the service and a reason to choose you.

3.2 1 page title(s) are too short or too long for search results

LOW

SEO & FINDABILITY · SEARCH FINDABILITY · 78%

The title is your headline in search results; a truncated or thin one lowers click-through even when you rank.

Observed: /service-page/1-testosterone-hormone-consultation (69 chars)

> **Recommended fix:** Aim for ~50–60 character titles leading with the service and location.

3.3 1 meta description(s) are outside the ideal length

LOW

SEO & FINDABILITY · SEARCH FINDABILITY · 76%

A well-sized description is the ad copy under your search result; off-length ones get replaced by random page text.

Observed: /service-page/1-testosterone-hormone-consultation (506 chars)

> **Recommended fix:** Write 140–160 character descriptions summarizing the page and a reason to click.

4 Local SEO & business info

1 finding

The business details a search engine uses to place you on a map and in local results.

> Inconsistent names, addresses or phone numbers across your own pages give local search conflicting answers about who and where you are.

4.1 Business structured data is missing key fields

LOW

SEO & FINDABILITY · LOCAL SEO & BUSINESS INFO · 78%

Partial schema gets partial benefit; completing name/address/phone/hours maximizes eligibility for enhanced local search results.

Observed: present: name, address, url

> **Recommended fix:** Add the missing fields (telephone, hours) to the LocalBusiness JSON-LD, matching your Google Business Profile.

5 Conversion & trust

1 finding

The signals on a page that tell a visitor this is a real business they can act with.

> People decide whether to contact you before they decide whether to trust you. Missing contact routes and trust signals end that decision early.

5.1 No tap-to-call phone link detected

LOW

SEO & FINDABILITY · CONVERSION & TRUST · 65%

For local practices the phone is the top conversion path; a non-clickable number adds friction on mobile.

Observed: no tel: links found

> **Recommended fix:** Make the header phone number a tel: link so phones dial on tap.

Security posture Moderate risk

What your site tells the outside world about how it is configured — observed without touching it. **11 observations in this discipline.**

6 Security headers

7 findings

Instructions your site gives a browser about what it is allowed to do.

> These are the settings that limit what injected or third-party code can get away with. They cost nothing to set and are checked by everyone who reviews you.

6.1 No Content-Security-Policy — injected scripts run unrestricted

MEDIUM

WEBSITE SECURITY · SECURITY HEADERS · 98%

A Content-Security-Policy tells the browser which sources of code are allowed to run on your pages. Without one, any script that gets onto a page — through a compromised third-party tool, for example — runs with full access to it.

Observed: no content-security-policy via response header or <meta http-equiv>

> **Recommended fix:** Add a Content-Security-Policy header. Start in report-only mode so you can see what it would block before it blocks anything.

6.2 Pages leak their full address to outside services (no Referrer-Policy)

MEDIUM

WEBSITE SECURITY · SECURITY HEADERS · 95%

Page addresses can describe sensitive interests; combined with trackers, third parties receive both who the visitor is and what they were reading.

Observed: no referrer-policy via response header or <meta name="referrer">

> **Recommended fix:** Set Referrer-Policy: strict-origin-when-cross-origin so outside services see only the domain.

6.3 1 session cookie(s) missing security flags

MEDIUM

WEBSITE SECURITY · SECURITY HEADERS · 84%

Session cookies are missing the flags that stop them being read over an unencrypted connection or by scripts on the page. A session cookie is what keeps someone signed in.

Observed: XSRF-TOKEN (missing HttpOnly)

> **Recommended fix:** Set Secure, HttpOnly and SameSite on session cookies.

6.4 Pages can be invisibly embedded in other sites (clickjacking)

LOW

WEBSITE SECURITY · SECURITY HEADERS · 97%

Your pages can be loaded invisibly inside someone else's site, which is how visitors are tricked into clicking something other than what they think they are clicking.

Observed: response header x-frame-options: absent

> **Recommended fix:** Send a frame-ancestors directive (or X-Frame-Options) so only sites you name can embed your pages.

6.5 HTTPS is enforced only weakly (HSTS present but limited)

LOW

WEBSITE SECURITY · SECURITY HEADERS · 90%

HSTS only protects for as long as its max-age, and only the hosts it covers. A short window or missing includeSubDomains leaves a first-connection downgrade window on the main domain or its subdomains.

Observed: strict-transport-security: max-age=31556952

> **Recommended fix:** Set Strict-Transport-Security to max-age=31536000; includeSubDomains (and add preload once verified).

6.6 No Permissions-Policy — embedded code can request camera, mic, location

LOW

WEBSITE SECURITY · SECURITY HEADERS · 88%

Without a Permissions-Policy, embedded third-party code can ask the browser for the camera, microphone or location on your behalf. The prompt appears to come from your site.

Observed: response header permissions-policy: absent

> **Recommended fix:** Add a Permissions-Policy header that turns off the capabilities your site does not use. Anything you do not name is left available.

6.7 Third-party scripts load without integrity verification (1 source) — LOW

WEBSITE SECURITY · SECURITY HEADERS · 76%

Scripts loaded from other companies run with the same access as your own code, and nothing checks that the file you received is the file you expected. If that vendor is compromised, the change arrives on your site automatically.

Observed: browser.sentry-cdn.com

> **Recommended fix:** Add integrity attributes to third-party scripts so the browser refuses a file that has been altered, and drop any you no longer use.

7 Email security — 2 findings

Whether your domain tells the world who is allowed to send email as you.

> Without these records, anyone can send mail that appears to come from your domain, and your own legitimate mail is more likely to land in spam.

7.1 DMARC is in monitor-only mode (p=none) — forgeries still get delivered — MEDIUM

WEBSITE SECURITY · EMAIL SECURITY · 88%

Monitor-only is the right first step, but left there permanently it provides no protection against spoofed email.

Observed: v=DMARC1; p=none; rua=mailto:contact@example.com

> **Recommended fix:** After reviewing DMARC reports, raise the policy to p=quarantine (then p=reject).

7.2 SPF is set to softfail (~all) rather than fail (-all) — LOW

WEBSITE SECURITY · EMAIL SECURITY · 90%

Your domain tells receiving mail servers to accept messages that fail the sender check rather than reject them, which weakens the protection to close to nothing.

Observed: v=spf1 include:_spf.google.com ~all

> **Recommended fix:** Change the SPF record from ~all to -all once you are confident every legitimate sender is listed.

8 DNS & certificate control — 1 finding

Who is allowed to answer for your domain name and issue certificates in your name.

> These records decide whether someone else can point your address somewhere they control, or obtain a valid certificate for it. Both are registrar-level settings.

8.1 No CAA record — any certificate authority can issue certs for example-practice.com

LOW

WEBSITE SECURITY · DNS & CERTIFICATE CONTROL · 72%

CAA is a cheap guard against certificate mis-issuance — if an attacker tricks some CA into issuing a cert for your domain, CAA can block it. One DNS record.

Observed: no CAA record for example-practice.com

> **Recommended fix:** Add a CAA record naming your certificate authority (e.g. "0 issue \"letsencrypt.org\"").

9 Transport security

1 finding

Whether the connection between your visitors and your site is properly encrypted.

> An unencrypted or downgradeable connection can be read or altered in transit on any shared network. It is also the single most visible security fact about your site.

9.1 HTTP compression is enabled on a page that carries a login form

LOW

WEBSITE SECURITY · TRANSPORT SECURITY · 62%

This is the precondition for BREACH, an attack that recovers secrets — session tokens, CSRF tokens — from a compressed response by measuring how its size changes with attacker-chosen input. It is a PRECONDITION, not a demonstrated vulnerability: the attack also needs a secret reflected in the response body and the ability to inject input into it, neither of which a cold external scan can confirm. Reported at low confidence for that reason.

Observed: content-encoding: br; login surface observed at /, /services, /contact

> **Recommended fix:** Verify whether authenticated responses reflect CSRF or session tokens into the body. If they do, disable compression for those specific responses (not site-wide) or mask the tokens per-request. Keep compression everywhere else — turning it off globally is the wrong fix.

Accessibility High risk

Whether people using a keyboard, a screen reader, or a phone can complete what your site is for. **6 observations in this discipline.**

Technical score 22/100 — ranks your own scans against each other, not a grade against other sites.

10 Navigation & links

2 findings

Whether every control can be reached and understood without a mouse.

> A link or button that cannot be reached by keyboard, or whose purpose is only clear from its position, ends the visit for the person who hit it.

Regulatory context for this area: ADA Title III website-accessibility suits run in the thousands a year: 3,117 were filed in federal court in 2025, up 27% on 2024 (Seyfarth Shaw ADA Title III tracker, published March 2026). Retail dominates those filings and healthcare is a small share of them, but the defects cited are the same ones listed here. The settled obligation for practices is HHS's Section 504 rule: WCAG 2.1 Level A and AA for the websites and apps of providers receiving federal financial assistance (Medicare/Medicaid), with compliance dates of May 11, 2027 for recipients with 15 or more employees and May 10, 2028 for smaller ones after a May 2026 interim final rule.

10.1 Links with no accessible name on 4 page(s)

HIGH

ACCESSIBILITY (ADA) · NAVIGATION & LINKS · 88% CONFIDENCE

A link that a screen reader announces as only “link” tells the person nothing about where it goes, so they cannot follow it. Icon-only links are the usual cause, and they are often the main navigation.

Observed: / (6 link(s)) · /services (6 link(s)) · /contact (6 link(s)) · /service-page/1-testosterone-hormone-consultation (6 link(s))

> **Recommended fix:** Add aria-label (or visually-hidden text) to icon-only links describing the destination.

10.2 Buttons with no accessible name on 4 page(s)

HIGH

ACCESSIBILITY (ADA) · NAVIGATION & LINKS · 84% CONFIDENCE

A control that announces only “button” cannot be used by someone who cannot see it. These are usually the menu, search and close controls — the ones every visit depends on.

Observed: / (1) · /services (2) · /contact (1) · /service-page/1-testosterone-hormone-consultation (1)

> **Recommended fix:** Add an aria-label to icon-only buttons describing the action ("Open menu", "Close", "Search").

11 Form accessibility

1 finding

Whether your forms can be completed by someone not using a mouse or a screen.

> A form is where visits turn into enquiries. A field with no label is a field a screen reader cannot announce, so the enquiry never arrives.

Regulatory context for this area: as in section 10 above.

11.1 Form fields without labels on 1 page(s) — unusable with a screen reader

HIGH

ACCESSIBILITY (ADA) · FORM ACCESSIBILITY · 85% CONFIDENCE

A form is where a visit turns into an enquiry. A field with no label is announced as “edit text”, so someone using a screen reader cannot tell which box wants their phone number — and the enquiry never arrives.

Observed: /contact (1 field(s))

> **Recommended fix:** Associate every field with a visible <label for=...> (or aria-label where a visible label is impossible); placeholders alone do not count.

12 Screen-reader structure

2 findings

Whether the page makes sense when it is read aloud instead of looked at.

> Headings, labels and landmarks are how someone using a screen reader navigates. Without them the page is one long undifferentiated block.

Regulatory context for this area: as in section 10 above.

12.1 Images missing alt text on 1 page(s) — MEDIUM

ACCESSIBILITY (ADA) · SCREEN-READER STRUCTURE · 85%

An image with no text alternative is silent to a screen reader and invisible to image search. Where the image carries the meaning — a price list, a map, a product — that meaning is simply missing for those visitors.

Observed: /services (7 imgs)

> **Recommended fix:** Add concise alt text to meaningful images and empty alt="" to decorative ones.

12.2 Heading levels skip on 4 page(s) — LOW

ACCESSIBILITY (ADA) · SCREEN-READER STRUCTURE · 78%

Headings are how someone using a screen reader skims a page. When levels skip, the page reads as one undifferentiated block — and search engines read the same structure.

Observed: / [1>3>2>3>2>6>6>6>6>6>6>6>3>2>6>6>6], /services [3>1>3>3>3>3>3>3>3>2>2], /contact [3>1>1>3>3>3>3], /service-page/1-testosterone-hormone-consultation [1>2>3>2>5>5>5>5>5>5>2]

> **Recommended fix:** Use heading levels in sequence without skipping (H1→H2→H3).

13 ● Accessibility posture — 1 finding

What your site publishes about its own accessibility, and how it is set up.

> A stated accessibility position is what a customer, a procurement reviewer or a complainant looks for first. Its absence is noticed before any specific defect is.

Regulatory context for this area: as in section 10 above.

13.1 No accessibility statement page — LOW

ACCESSIBILITY (ADA) · ACCESSIBILITY POSTURE · 70%

A statement doesn't fix defects, but it documents good-faith effort, gives affected users a remediation channel before a lawyer does, and is cheap insurance.

Observed: no accessibility link among homepage/footer links

> **Recommended fix:** Publish an accessibility statement (conformance target, known limitations, contact for assistance) linked from the footer.

Speed & mobile Low risk

How heavy your pages are to load, measured in the lab — not from your real visitors. **1 observation in this discipline.**

Technical score 96/100 — ranks your own scans against each other, not a grade against other sites.

14 Speed & mobile

1 finding

How much work a page makes a device do before it is usable — measured in our lab, not from your visitors.

> Weight and blocking work delay the moment a page can be used. You pay for the click whether or not the visitor waits for the page.

14.1 32 image(s) have no width/height attributes

LOW

SEO & FINDABILITY · SPEED & MOBILE · 84%

This is a direct cause of layout shift: text renders, then an image loads and shoves it down the page — often just as someone is about to tap a button. Cumulative Layout Shift is one of the three Core Web Vitals Google uses in ranking, and dimension attributes are the cheapest fix for it.

Observed: / (14), /services (10), /contact (5), /service-page/1-testosterone-hormone-consultation (3)

> **Recommended fix:** Add width and height attributes (or an aspect-ratio CSS rule) to every <img> so the browser can reserve the space.

4 Methodology & depth

How deep we scanned

75	3,000+	6	Full
CHECKS RUN	KNOWN TRACKERS SCREENED	ANALYSIS LENSES	PAGE CAPTURE

Beyond a cookie scan, we inspect every outbound channel — requests, form-field values, beacons, WebSockets, cookies and browser-storage writes — and match what we find against our live database of FDA, FTC, DOJ and state enforcement actions and court cases, updated continuously. The itemized breakdown of the **75** checks is in *What we checked* below.

Benchmarked against the standard tools

For each pillar, a detector for every defect class the recognized reference tools can find — verified check-by-check against the same rule catalog, on the same page.

PILLAR	REFERENCE TOOL	COVERAGE	…AND BEYOND
Accessibility a detector for every WCAG A/AA rule these engines run, proven on the same page	axe-core	66/66	each check mapped to its WCAG 2.2 success criterion (15 SCs, incl. Target Size — new in 2.2)
	Google Lighthouse (Accessibility)	57/57	the manual/unscored audits Lighthouse only links out for, we either check or skip with a documented reason
	IBM Equal Access	122/123	1 gap named, not hidden (form colour-only cues); the 2 skips are IBM MANUAL-REVIEW rules no automated tool decides
	HTML CodeSniffer	11/11	two error classes axe and Lighthouse leave to manual review — empty headings, fieldsets without a legend — we now detect
Security measured against the hardest public standards test, with every remaining gap named	Internet.nl	19/27	we see 22 of 27 and escalate 19 — the other 3 are reported as evidence, not flagged. The 5 true gaps are all TLS-handshake depth, 2 of them measured INFEASIBLE in pure Node (RC4/3DES are compiled out of OpenSSL upstream; tls.connect exposes no early-data surface)
	Mozilla Observatory	9/9	21 checks Observatory does not run — TLS configuration, known-CVE libraries, SPF/DKIM/DMARC, DNSSEC/CAA
	securityheaders.com	6/6	we grade each header’s strength, not just its presence (weak CSP, short-max-age HSTS)
	SSL Labs	5/5	we grade the same TLS config offline (protocol, key exchange, cipher, certificate, HSTS) without a remote scan
	retire.js + OSV.dev	✓	we bundle both databases and detect their advisories by filename and by the runtime version a library exposes — recall a filename-only scan misses

PILLAR	REFERENCE TOOL	COVERAGE	...AND BEYOND
Privacy every tracking behavior these inspectors report, proven against the same site	Blacklight	11/11	each tracker tied to the enforcement action it appeared in — context Blacklight does not carry
	Disconnect	5/5	we already bundle the list and detect by category — advertising, analytics, social, content, fingerprinting
	WhoTracks.me	5/5	we bundle it (5,089 domains) and use its owner data to name who each tracker belongs to
	DuckDuckGo Tracker Radar	11/11	its non-tracking categories (CDN, payment, SSO, badges) are correctly not flagged — precision, not blind spots
SEO a detector for every Lighthouse SEO audit and every Screaming Frog issue family	Google Lighthouse (SEO)	11/11	Google's open web-quality auditor
	Screaming Frog SEO Spider	121/133	12 remaining gaps are itemised, not hidden: all need whole-site crawl state (orphans vs sitemap, near-duplicate clustering, cross-page link-graph reads)
Performance every Core Web Vital Google ranks on, from real-user field data	Google CrUX (Core Web Vitals)	5/5	plus lab load time, page weight, image weight and mobile readiness
	Google Lighthouse (Performance)	21/23	2 remaining gaps named, not hidden (duplicate JS, legacy JS) — both need bundle-content diffing, not a trace
Claims & Trust the one pillar no scanner competes on — measured against the real enforcement record	FTC / FDA / DOJ enforcement corpus	✓	each finding matched to the enforcement action pattern it resembles

Capability coverage means a detector exists for each defect class the reference tool can detect — verified check-by-check on the same page. It is not a claim of identical scoring, and for accessibility it is the machine-detectable subset of WCAG (~30–50% of the standard).

Third-party inventory

2 distinct third parties observed loading on this site (0 recognized, 2 unrecognized).

VENDOR	PAGES	HOW DATA WAS SENT	VENDOR AGREEMENT
UNRECOGNIZED (2)			
parastorage.com unrecognized	1	requests pre-consent	—
wixstatic.com unrecognized	1	requests pre-consent	—

Vendor terms as of June 2026. "Vendor agreement" reflects our verify-framed record of a vendor's standard terms where we have one — a blank means verify the vendor's terms yourself; it is not a statement that a BAA is unavailable. Unrecognized parties are listed honestly; they are not matched to our catalog.

What we checked

75 checks ran across 4 pages; **55** found no issue, **20** raised a finding:

Regulated-data privacy 1 flagged · 19 checked clean

✓ Advertising pixels on sensitive pages
✓ Personal identifiers observed in transit
✓ Session recording / heatmap tools
✓ Customer-data-platform server-side fan-out
✓ Device fingerprinting (by vendor and by technique)
✓ Persistent identifiers in browser storage
✓ Cross-network cookie syncing
✓ CNAME-cloaked (first-party-disguised) trackers
✓ Third-party WebSocket data streams
✓ Third-party asset leakage on sensitive pages
✓ Form submission destinations & encryption
✓ Sensitive data in page addresses
✓ Embedded chat / scheduling / form widgets
✓ Tracking cookies vs consent timing
✓ Consent enforcement (does Decline stop tags)
✓ Global Privacy Control signal honored
✓ Trackers that fire only on some devices
• Site-platform vendor-agreement posture
✓ Privacy policy present while collecting data
✓ Separate consumer-health-data policy

Visitor privacy 12 checked clean

✓ Third-party trackers & advertising pixels
✓ Personal data observed leaving the browser
✓ Session recording / heatmap tools
✓ Device fingerprinting
✓ Cookie lifetime & third-party-set first-party cookies
✓ Privacy policy present & consistent with observed behavior
✓ Sale/share opt-out control actually present
✓ Tracking cookies vs consent timing
✓ Connections opened to third parties before consent
✓ High-value pages the site excluded from scanning
✓ Tracking on the error/404 template
✓ Where forms send what visitors type

Website security 8 flagged · 4 checked clean

• TLS certificate, protocol version & cipher strength
• HSTS / transport hardening
• Content-Security-Policy
• Security response headers
✓ Cross-origin resource sharing (CORS)
• Subresource integrity on third-party scripts
• Secure / HttpOnly cookie flags
✓ JavaScript libraries with published vulnerabilities
✓ Published security contact (security.txt)
✓ Server software version disclosure
• Email authentication (SPF / DKIM / DMARC)
• DNS hardening (DNSSEC / CAA)

SEO & findability 6 flagged · 8 checked clean

- ● Title & meta-description quality
- ● Heading structure & H1
- ✓ Canonical, robots & indexability
- ✓ Sitemap presence & health
- ● Structured data (schema.org)
- ● Content depth, duplication & internal linking
- ● Local business info (NAP)
- ✓ Link health, anchor text & crawlability
- ✓ URL structure & tracking parameters
- ✓ International targeting (hreflang)
- ✓ Page head & resource hygiene
- ✓ AI crawler access (retrieval vs training)
- ✓ Raw vs rendered HTML (JavaScript dependence)
- ● Image markup (alt text, dimensions)

Performance 7 checked clean

- ✓ Core Web Vitals (field data)
- ✓ Page & image weight
- ✓ Render-blocking resources & font loading
- ✓ Caching, protocol version & back/forward cache
- ✓ Third-party request weight & DOM size
- ✓ Mobile viewport & responsiveness
- ✓ HTTPS redirect

Accessibility (ADA) 5 flagged · 4 checked clean

- ● Image & SVG alternative text
- ● Form field labels & grouping
- ✓ Color contrast & colour-only cues
- ● Landmarks, headings & skip links
- ● ARIA, accessible names & focus order
- ✓ Zoom, target size & text spacing
- ✓ Media captions & autoplay
- ✓ Data table headers
- ● Accessibility statement

Trust & substantiation 1 checked clean

- ✓ Unsubstantiated marketing claims

A read-only scan of observable behavior: we identified our crawler honestly and honored robots directives. Detection matches a known-vendor catalog (vendor terms as of June 2026), so absence of a finding is not proof a site is free of a given issue. Engine v0.2.0.

A Appendices

Appendix — URLs Scanned

These results bind to exactly the 4 URLs below, as they existed on August 19, 2026 (engine v0.2.0). Pages not listed were not examined.

- https://example-practice.com
- https://www.example-practice.com/services
- https://www.example-practice.com/contact
- https://www.example-practice.com/service-page/1-testosterone-hormone-consultation

Appendix — Evidence record

A per-finding record of what was observed, on which pages, over which channels — captured August 19, 2026 by engine v0.2.0 on a read-only scan. Each item can be re-observed independently (see *Verify this yourself*). Raw request/identifier values are in the evidence CSV export. This documents our capture process and is not a legal conclusion.

HIGH **Links with no accessible name on 4 page(s)** `a11y-empty-links`

Observed: / (6 link(s)) · /services (6 link(s)) · /contact (6 link(s)) · /service-page/1-testosterone-hormone-consultation (6 link(s))

Where: see the observation above — pages not recorded individually in this scan

HIGH **Form fields without labels on 1 page(s) — unusable with a screen reader** `a11y-unlabeled-fields`

Observed: /contact (1 field(s))

Where: see the observation above — pages not recorded individually in this scan

HIGH **Buttons with no accessible name on 4 page(s)** `a11y-nameless-buttons`

Observed: / (1) · /services (2) · /contact (1) · /service-page/1-testosterone-hormone-consultation (1)

Where: see the observation above — pages not recorded individually in this scan

HIGH **Site runs on Wix; its standard plan is not offered with a Business Associate Agreement (BAA) — verify before its forms collect protected health information (PHI)** `platform-baa-wix`

Observed: platform Wix (header x-wix-request-id; assets from static.parastorage.com; generator "Wix.com Website Builder"); 4 data-collection form(s) on 4 page(s); vendor-terms as of June 2026

Where: see the observation above — pages not recorded individually in this scan

MEDIUM **No Content-Security-Policy — injected scripts run unrestricted** `no-csp`

Observed: no content-security-policy via response header or <meta http-equiv>

Where: site-wide (a server/DNS setting, not a per-page fact)

MEDIUM **Pages leak their full address to outside services (no Referrer-Policy)** `no-referrer`

Observed: no referrer-policy via response header or <meta name="referrer">

Where: site-wide (a server/DNS setting, not a per-page fact)

MEDIUM **DMARC is in monitor-only mode (p=none) — forgeries still get delivered** `email-dmarc-none`

Observed: v=DMARC1; p=none; rua=mailto:contact@example.com

Where: site-wide (a server/DNS setting, not a per-page fact)

MEDIUM **Images missing alt text on 1 page(s)** `a11y-alt`

Observed: /services (7 imgs)

Where: see the observation above — pages not recorded individually in this scan

MEDIUM **1 session cookie(s) missing security flags** `insecure-cookies`

Observed: XSRF-TOKEN (missing HttpOnly)

Where: see the observation above — pages not recorded individually in this scan

MEDIUM **1 page(s) have very little text content** `seo-thin`

Observed: /contact (135w)

Where: see the observation above — pages not recorded individually in this scan

LOW **Pages can be invisibly embedded in other sites (clickjacking)** `no-xfo`

Observed: response header x-frame-options: absent

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **HTTPS is enforced only weakly (HSTS present but limited)** `hsts-weak`

Observed: strict-transport-security: max-age=31556952

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **SPF is set to softfail (~all) rather than fail (-all)** `email-spf-soft`

Observed: v=spf1 include:_spf.google.com ~all

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **No Permissions-Policy — embedded code can request camera, mic, location** `no-permissions-policy`

Observed: response header permissions-policy: absent

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **75% of pages lack a meta description** `seo-missing-meta`

Observed: /, /services, /contact

Where: see the observation above — pages not recorded individually in this scan

LOW **Images missing alt text on 1 page(s)** `seo-alt`

Observed: /services (7 imgs)

Where: see the observation above — pages not recorded individually in this scan

LOW **32 image(s) have no width/height attributes** `seo-image-no-dimensions`

Observed: / (14), /services (10), /contact (5), /service-page/1-testosterone-hormone-consultation (3)

Where: see the observation above — pages not recorded individually in this scan

LOW **Heading levels skip on 4 page(s)** `seo-heading-order`

Observed: / [1>3>2>3>2>6>6>6>6>6>6>6>3>2>6>6>6], /services [3>1>3>3>3>3>3>3>3>3>2>2], /contact [3>1>1>3>3>3>3>3], /service-page/1-testosterone-hormone-consultation [1>2>3>2>5>5>5>5>5>5>2]

Where: see the observation above — pages not recorded individually in this scan

LOW **1 page(s) have a missing or duplicated main heading (H1)** `seo-h1`

Observed: /contact (2)

Where: see the observation above — pages not recorded individually in this scan

LOW **1 page title(s) are too short or too long for search results** `seo-title-length`

Observed: /service-page/1-testosterone-hormone-consultation (69 chars)

Where: see the observation above — pages not recorded individually in this scan

LOW **Business structured data is missing key fields** `seo-schema-incomplete`

Observed: present: name, address, url

Where: see the observation above — pages not recorded individually in this scan

LOW **Heading levels skip on 4 page(s)** `a11y-heading-order`

Observed: / [1>3>2>3>2>6>6>6>6>6>6>6>3>2>6>6>6], /services [3>1>3>3>3>3>3>3>3>3>2>2], /contact [3>1>1>3>3>3>3], /service-page/1-testosterone-hormone-consultation [1>2>3>2>5>5>5>5>5>5>2]

Where: see the observation above — pages not recorded individually in this scan

LOW **Third-party scripts load without integrity verification (1 source)** `no-sri`

Observed: browser.sentry-cdn.com

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **1 meta description(s) are outside the ideal length** `seo-meta-length`

Observed: /service-page/1-testosterone-hormone-consultation (506 chars)

Where: see the observation above — pages not recorded individually in this scan

LOW **No CAA record — any certificate authority can issue certs for example-practice.com** `dns-no-caa`

Observed: no CAA record for example-practice.com

Where: site-wide (a server/DNS setting, not a per-page fact)

LOW **No accessibility statement page** `a11y-no-statement`

Observed: no accessibility link among homepage/footer links

Where: see the observation above — pages not recorded individually in this scan

LOW **No tap-to-call phone link detected** `seo-no-tap-phone`

Observed: no tel: links found

Where: see the observation above — pages not recorded individually in this scan

LOW **HTTP compression is enabled on a page that carries a login form** `tls-http-compression`

Observed: content-encoding: br; login surface observed at /, /services, /contact

Where: site-wide (a server/DNS setting, not a per-page fact)

Recommended next steps

We can remediate the 28 items identified above, prioritizing the 4 highest-priority issues. To receive a prioritized remediation plan with timeline, reply to this report.

This is a point-in-time automated technical scan of observable website behavior on the specific URLs scanned, as they existed at the scan date shown — not a legal compliance audit or attestation, and not an audit, certification, or compliance opinion of any kind. Results describe only the pages scanned at that time; they are not an assessment of the business or entity operating the site, and must not be represented as current after the scan date. A "pass" means no high-priority technical issues were found at the scan threshold on the pages crawled — it does not certify HIPAA, ADA, or any regulatory compliance, and does not cover items unobservable from outside (signed vendor agreements, server configuration, internal policies). Form analysis covers each form's declared submission target; forms that submit via JavaScript to endpoints not visible in the page markup are not assessed. Third-party/tracker detection matches a known-vendor catalog, so absence of a finding is not proof a site is free of trackers. This report is general information about observable technical facts and is not legal advice, does not create an attorney-client or other professional relationship, and is not a substitute for review by a qualified attorney. For your specific legal obligations, consult an attorney licensed in your jurisdiction.

Full report · Assessment completeness: complete · Reference: · Generated by ClearSite