Plumb

WEB COMPLIANCE AUDIT REPORT · TWO-PART DELIVERABLE

Compliance audit for your website

https://cascadevalleyhealth.example/

PAGES AUDITED	CRITICAL	SERIOUS	TOTAL FINDINGS
24	8	10	23

+ 3 informational findings on third-party redirect targets (detail in Part 2)

AUDIT PREPARED FOR cascadevalleyhealth.example	GENERATED BY Plumb
STANDARD WCAG22AA	SCOPE 24 of 41 discovered
GENERATED Apr 15, 2026 UTC	AUDIT ID 5a3f8b2e

AI-augmented automated audit — not legal advice or a certification. Web-layer checks only; organizational controls (access reviews, change management) are out of scope.

TABLE OF CONTENTS

What's in this report

This report is delivered in two parts so the right information lands with the right audience. 83 total findings across 24 audited pages.

PART 1 OF 2

Executive brief

For leadership, legal, and functional managers

Read this part to understand what's wrong, how exposed your organization is, and which fixes deliver the most risk reduction first. No code, no rule IDs — just plain-English findings, regulatory context, and a prioritized roadmap. Hand Part 2 to your engineering team.

SECTION 1.1

Executive summary

We audited **24** pages on **https://cascadevalleyhealth.example/** (sampled from 41 discovered) against WCAG 2.2 Level AA and seven adjacent compliance domains. We found **23** findings on your site, of which **8** are critical and **10** are serious. An additional **3** informational findings were captured on third-party redirect targets (auth providers, embeds, etc.) — listed in Part 2 for completeness, not counted in the headline because your team cannot fix them.

CRITICAL	SERIOUS	MODERATE	MINOR
8	10	5	0

Third-party redirect findings (informational): 1 critical, 2 serious, 0 moderate, 0 minor. Detail in Part 2.

PAGES AUDITED	AI-AUGMENTED FINDINGS	NON-ACCESSIBILITY	AUDIT DURATION
24	5	10	22 min

What this site does

Cascade Valley Health is a regional health system operating across 6 facilities in the Pacific Northwest. The site serves three audiences: prospective patients researching providers and services, current patients managing appointments and bills, and referring physicians looking up specialists. Critical conversion paths include the patient portal sign-in (existing patients), the appointment scheduler (new patients), and the find-a-doctor directory (both audiences). The brand uses a navy/teal palette with prominent imagery of providers and facilities.

What we found

The Cascade Valley Health website has 71 WCAG 2.2 conformance violations across 24 audited pages. 8 are critical and concentrated in three high-stakes flows: patient portal sign-in, appointment scheduling, and the find-a-doctor directory.

The most important issue: the patient portal sign-in requires CAPTCHA-style cognitive transcription with no alternative, which violates WCAG 2.2's new Accessible Authentication criterion. Patients with cognitive disabilities, low vision, or low literacy are effectively locked out of their own medical records. This is both a high legal-risk finding and a serious patient-care issue. We recommend immediate prioritization.

Beyond authentication, the audit found systemic patterns: color contrast on the site's primary CTA blue (#6BA4D9 on white) fails 1.4.3 across the marketing pages, and provider availability is conveyed using color-only status dots in the find-a-doctor directory. Both are fixable with site-wide changes rather than page-by-page work.

The organization is well-positioned to remediate: most findings cluster around a small number of design-system primitives (CTA buttons, doctor-card components, form inputs). Fixing the design system once will

resolve dozens of individual violations.

> **How to use this report:** Part 1 (this section) is the executive view — what's wrong, why it matters, and which fixes go first. Part 2 is the engineering view — every affected element, every page, with before/after code your team can apply directly.

SECTION 1.2

Compliance scorecard

One card per compliance domain. The dot is a quick traffic light; the line beneath it explains what was checked and what's outstanding.

Accessibility (WCAG / ADA)

11 critical or serious findings

Whether people using screen readers, keyboard navigation, or other assistive technology can use the site. Falls under ADA Title III and Section 508 in the US.

15 total findings in this domain.

HTTP security headers

2 critical or serious findings

The browser-level protections that prevent clickjacking, cross-site scripting injection, and traffic downgrade. Baseline expected by every modern web platform.

2 of 6 checks failed.

Privacy disclosure (CCPA / CPRA)

1 critical or serious finding

Whether the site presents a privacy policy and offers California residents the rights they are entitled to (do-not-sell, limit-use-of-sensitive-info, etc.).

2 of 5 checks failed.

Cookie consent & trackers

1 critical or serious finding

Whether the third-party trackers that load (analytics, ad pixels, session replay) are gated behind a clear consent banner with a working reject option.

2 of 3 checks failed.

Core Web Vitals

1 critical or serious finding

Google's page-experience signals (LCP, INP, CLS). Poor scores are a documented ranking-signal demotion and a leading driver of bounce.

2 of 7 checks failed.

HIPAA (web component)

1 critical or serious finding

For sites that touch protected health information: whether PHI ever appears in URLs, whether PHI forms are encrypted and POST-only, whether browser autofill can leak PHI.

2 of 6 checks failed.

PCI-DSS (web component)

Clean

For sites that accept card payments: whether checkout is HTTPS-only, whether payment forms use tokenized iframes, whether the merchant has minimized SAQ-A scope.

All 6 checks passed.

FERPA (web component)

Clean

For sites that handle student records: whether student PII is exposed in URLs, whether forms protect the data, whether HTTPS is enforced.

All 5 checks passed.

SOC 2 (web-verifiable evidence)

1 critical or serious finding

Audit evidence for the subset of SOC 2 Trust Service Criteria that can be verified externally from a website (CC6.6 boundary protection, CC6.7 restricted transmission, CC6.8 malicious software prevention, CC9.1 risk mitigation).

3 of 4 checks failed.

Standards mapping

Cross-walk of every WCAG 2.x criterion that fired on this scan to its Section 508 (US federal) chapter/section. Use this when a federal or public-sector buyer asks "are you Section 508 conformant?" — the answer is "yes against rows showing Pass, and these specific 12 criteria need remediation." Sorted by worst-severity, then by element count.

WCAG CRITERION	NAME	WORST SEVERITY	ELEMENTS	LEVEL	SECTION 508
4.1.2	Name, role, value	CRITICAL	4	A	502.3.6 / 502.3.7
1.4.3	Contrast (minimum)	CRITICAL	2	AA	502.3.1
1.1.1	Non-text content	CRITICAL	2	A	502.3.1 / 501.1
1.3.1	Info and relationships	CRITICAL	2	A	502.3.1
3.3.8	Accessible authentication (minimum)	CRITICAL	1	AA	502.3.1
2.4.4	Link purpose (in context)	SERIOUS	2	A	502.3.1
2.4.7	Focus visible	SERIOUS	1	AA	502.3.1
2.4.11	Focus not obscured (minimum)	SERIOUS	1	AA	502.3.1
2.5.8	Target size (minimum)	MODERATE	1	AA	502.3.1
1.4.1	Use of color	MODERATE	1	A	502.3.1
3.3.2	Labels or instructions	MODERATE	1	AA	502.3.1
3.3.3	Error suggestion	MODERATE	1	AA	502.3.1

Section 508 mappings reference the US Access Board's revised 2018 ICT standards (Chapter 5 — Software). Rows showing "—" are scan-detectable WCAG criteria without a direct 1:1 mapping in the 508 chapter we currently track; they still count toward WCAG / ADA conformance.

SECTION 1.3

Top risks & business impact

The findings below are ranked by composite risk: regulatory exposure × likelihood of detection × user impact. Each card explains what's at stake in business terms and how to think about prioritization. Detailed code-level remediation is in Part 2.

#1 Patient portal sign-in requires cognitive transcription with no alternative

CRITICAL

ACCESSIBILITY (WCAG / ADA) · AFFECTS PATIENT PORTAL SIGN-IN FLOW (1 PAGE, 1 ELEMENT — BUT BLOCKS ALL RETURNING PATIENTS)

LIKELIHOOD	IMPACT	COMPOSITE
High	High	Critical

BUSINESS IMPACT

Users with disabilities are blocked from completing core flows on your site. Beyond legal exposure, this is a direct revenue and reputation cost — abandoned conversions, abandoned support tickets, and the kind of customer experience that ends up on social media.

LEGAL & REGULATORY EXPOSURE

Direct ADA Title III exposure. Plaintiffs' firms scan public sites for exactly this pattern; settlement demands typically open at $10–50k per defendant. WCAG 2.2 added explicit criteria (Accessible Authentication, Focus Not Obscured, Target Size) that are now part of the diligence checklist.

USER EXPERIENCE IMPACT

The patient portal at /patient-portal requires users to transcribe distorted text from an image to sign in.

RECOMMENDATION

Add at least one alternative authentication method that does not rely on cognitive transcription: email-based magic link (lowest implementation cost), passkeys (best user experience), or third-party OAuth (Google, Apple). The existing CAPTCHA can remain as a bot-prevention layer if needed, but must not be the only path. We recommend magic-link first — it is a single back-end change, requires no client-side complexity, and works for every user with email access.

#2 Primary CTA blue (#6BA4D9) fails contrast on white backgrounds across the marketing site

CRITICAL

ACCESSIBILITY (WCAG / ADA) · AFFECTS 18 INSTANCES ACROSS 14 PAGES — EVERY "BOOK AN APPOINTMENT", "FIND A DOCTOR", AND "LEARN MORE" BUTTON

LIKELIHOOD	IMPACT	COMPOSITE
High	High	Critical

BUSINESS IMPACT

Users with disabilities are blocked from completing core flows on your site. Beyond legal exposure, this is a direct revenue and reputation cost — abandoned conversions, abandoned support tickets, and the kind of customer experience that ends up on social media.

LEGAL & REGULATORY EXPOSURE

Direct ADA Title III exposure. Plaintiffs' firms scan public sites for exactly this pattern; settlement demands typically open at $10–50k per defendant. WCAG 2.2 added explicit criteria (Accessible Authentication, Focus Not Obscured, Target Size) that are now part of the diligence checklist.

USER EXPERIENCE IMPACT

The CTA blue used throughout the marketing site (#6BA4D9) achieves only 2.94:1 contrast against white backgrounds, well below the 4.5:1 required for normal text and the 3:1 required for UI components and large text.

RECOMMENDATION

Darken the brand CTA blue to #2563EB (or any blue achieving ≥4.5:1 against white). Update the design-system token cv-blue-primary in the source CSS; the change propagates to every CTA without per-component edits. Verify visually that the darker blue still reads as "primary action" against the navy header and the photo backgrounds in the hero rotator.

#3 Provider availability conveyed only by colored status dot

HIGH

ACCESSIBILITY (WCAG / ADA) · AFFECTS FIND-A-DOCTOR DIRECTORY (1 PAGE, 47 DOCTOR CARDS)

LIKELIHOOD	IMPACT	COMPOSITE
Low	High	High

BUSINESS IMPACT

Significant friction for users relying on assistive technology. Affected users will often complete the flow but more slowly or with errors, driving up support cost and harming satisfaction.

LEGAL & REGULATORY EXPOSURE

Material ADA Title III exposure. Courts and the DOJ both reference WCAG conformance; serious AA failures are routinely cited in demand letters.

USER EXPERIENCE IMPACT

In the find-a-doctor directory, each provider card shows a small colored dot indicating availability: green for "accepting new patients", gray for "not accepting".

RECOMMENDATION

Add a text label adjacent to the dot ("Accepting new patients" / "Not accepting"), or convert the dot into an icon-with-text component. The icon may stay for visual scanability but must be accompanied by accessible text.

#4 Doctor profile photos lack meaningful alt text site-wide

CRITICAL

ACCESSIBILITY (WCAG / ADA) · AFFECTS 47 PHOTOS ACROSS THE DOCTOR DIRECTORY; 9 PHOTOS ON INDIVIDUAL DOCTOR PROFILE PAGES

LIKELIHOOD	IMPACT	COMPOSITE
Low	High	Critical

BUSINESS IMPACT

Users with disabilities are blocked from completing core flows on your site. Beyond legal exposure, this is a direct revenue and reputation cost — abandoned conversions, abandoned support tickets, and the kind of customer experience that ends up on social media.

LEGAL & REGULATORY EXPOSURE

Direct ADA Title III exposure. Plaintiffs' firms scan public sites for exactly this pattern; settlement demands typically open at $10–50k per defendant. WCAG 2.2 added explicit criteria (Accessible Authentication, Focus Not Obscured, Target Size) that are now part of the diligence checklist.

USER EXPERIENCE IMPACT

Doctor profile photos render as <img> tags with no alt attribute (or an empty alt that is not the appropriate decorative pattern).

RECOMMENDATION

Because the doctor's name appears as adjacent text, the photos should be marked decorative with alt="". This avoids redundant announcement ("Dr. Sarah Chen, image of Dr. Sarah Chen"). On dedicated profile pages where the photo is the only identifier above the fold, use a descriptive alt instead.

#5 Form fields rely on placeholder text instead of labels

CRITICAL

ACCESSIBILITY (WCAG / ADA) · AFFECTS APPOINTMENT SCHEDULER (4 FIELDS), PATIENT PORTAL SIGN-IN (3 FIELDS), CONTACT FORM (2 FIELDS)

LIKELIHOOD	IMPACT	COMPOSITE
Low	High	Critical

BUSINESS IMPACT

Users with disabilities are blocked from completing core flows on your site. Beyond legal exposure, this is a direct revenue and reputation cost — abandoned conversions, abandoned support tickets, and the kind of customer experience that ends up on social media.

LEGAL & REGULATORY EXPOSURE

Direct ADA Title III exposure. Plaintiffs' firms scan public sites for exactly this pattern; settlement demands typically open at $10–50k per defendant. WCAG 2.2 added explicit criteria (Accessible Authentication, Focus Not Obscured, Target Size) that are now part of the diligence checklist.

USER EXPERIENCE IMPACT

Several form fields use HTML placeholder text as the only label.

RECOMMENDATION

Add a visible <label> element for every input. Placeholders may remain for format hints ("MM/DD/YYYY") but never as the primary label. If the visual design requires labels-as-placeholders, use a floating-label pattern with proper <label> markup underneath.

#6 Focus indicators removed without replacement; new sticky-header obscure issue

HIGH

ACCESSIBILITY (WCAG / ADA) · AFFECTS SITE-WIDE (EVERY PAGE) — FOCUS OUTLINE REMOVED IN GLOBAL CSS; STICKY HEADER OBSCURES FOCUSED ELEMENTS

LIKELIHOOD	IMPACT	COMPOSITE
High	High	High

BUSINESS IMPACT

Significant friction for users relying on assistive technology. Affected users will often complete the flow but more slowly or with errors, driving up support cost and harming satisfaction.

LEGAL & REGULATORY EXPOSURE

Material ADA Title III exposure. Courts and the DOJ both reference WCAG conformance; serious AA failures are routinely cited in demand letters.

USER EXPERIENCE IMPACT

The site CSS contains a:focus { outline: none; } site-wide without a visual replacement, leaving keyboard-only users unable to tell which element is focused.

RECOMMENDATION

Restore the focus outline with a clearly visible style (we suggest a 2px solid offset outline matching the brand accent color), and add scroll-padding-top to the html element equal to the sticky-header height so focused elements scroll into view above the header.

#7 Footer social-icon links fail target-size requirement (WCAG 2.2)

MODERATE

ACCESSIBILITY (WCAG / ADA) · AFFECTS SITE FOOTER — 6 SOCIAL ICONS ON EVERY PAGE

LIKELIHOOD	IMPACT	COMPOSITE
High	Medium	Moderate

BUSINESS IMPACT

Friction or non-conformance that degrades the experience for a smaller share of users. Resolving these elevates overall quality but is unlikely to be the single trigger for a complaint.

LEGAL & REGULATORY EXPOSURE

Limited direct exposure on its own, but moderate findings can stack with other issues in the same demand letter.

USER EXPERIENCE IMPACT

The footer social-media icons are 18×18 CSS pixels with 4px spacing between them.

RECOMMENDATION

Increase the click-target padding so each icon has at least a 24×24 hit area, OR keep the visual size and increase the spacing between icons to 24px. The visual icon size can stay at 18px — only the tappable area must change.

#8 Insurance "Plan code" field has no example or help text

MODERATE

ACCESSIBILITY (WCAG / ADA) · AFFECTS BILLING & INSURANCE FORM (1 PAGE, 1 FIELD — BUT HIGH ABANDONMENT DRIVER)

LIKELIHOOD	IMPACT	COMPOSITE
Low	Medium	Moderate

BUSINESS IMPACT

Friction or non-conformance that degrades the experience for a smaller share of users. Resolving these elevates overall quality but is unlikely to be the single trigger for a complaint.

LEGAL & REGULATORY EXPOSURE

Limited direct exposure on its own, but moderate findings can stack with other issues in the same demand letter.

USER EXPERIENCE IMPACT

The "Plan code" input on the billing form has no example value, no help link, no autocomplete from common providers, and no description of what format the code should take.

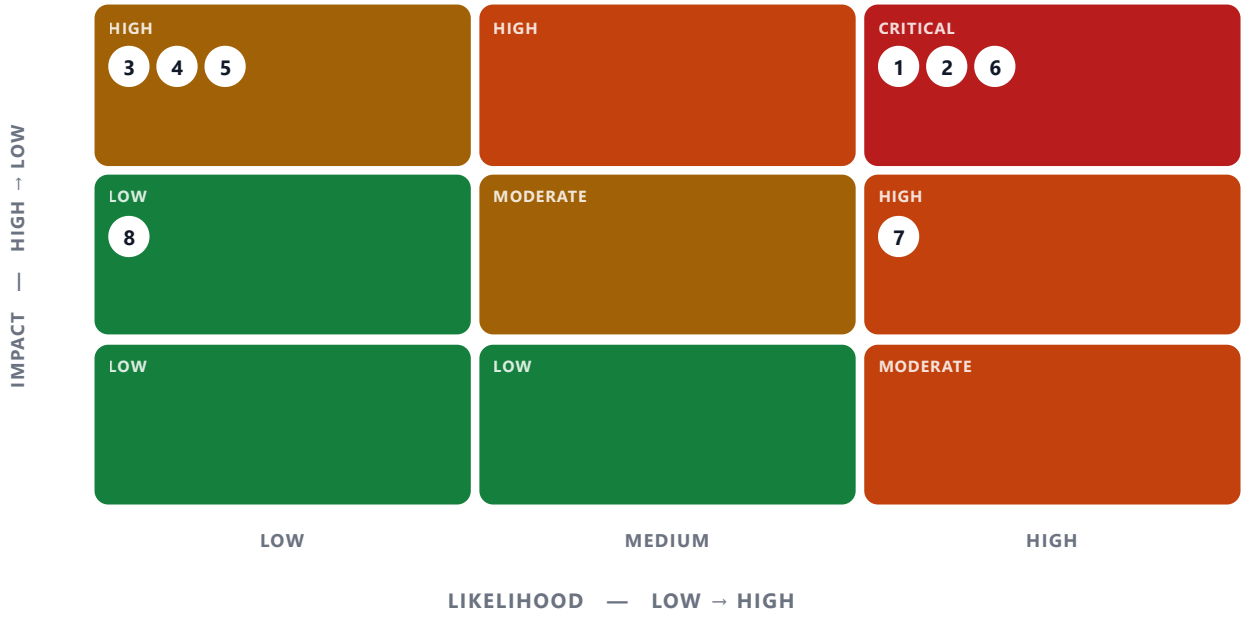
RECOMMENDATION

Add (1) a placeholder example like "Example: BCBS-PPO-2024", (2) a link to a help modal showing where to find the code on common insurance cards with images, and (3) ideally an "I don't know my plan code — look up by provider" alternative path.

SECTION 1.4

Risk matrix

Each numbered risk from the previous section is plotted by the likelihood it gets noticed by users or regulators (horizontal axis) against the impact if it does (vertical axis). The colored bands are the composite risk level.



Numbered dots match the **#N** on each card in section 1.3. Risks in the top-right quadrant (high impact, high likelihood) deserve first attention regardless of remediation effort.

SECTION 1.5

Recommended roadmap

Phased remediation plan based on the top risks. Phase 1 is the legal-and-user-impact bar — the items that justify a hotfix release. Phase 2 closes the moderate-risk gaps that would surface in a regulator inquiry. Phase 3 is the long tail that improves your overall posture.

1

Hotfix — 0 to 30 days 4 ITEMS

Address every critical finding. Most of these are individual element fixes or single configuration changes (security headers, autocomplete attributes) that can ship in one sprint.

#1	Patient portal sign-in requires cognitive transcription with no alternative	Patient portal sign-in flow (1 page, 1 element — but blocks all returning patients)
#2	Primary CTA blue (#6BA4D9) fails contrast on white backgrounds across the marketing site	18 instances across 14 pages — every "Book an appointment", "Find a doctor", and "Learn more" button
#4	Doctor profile photos lack meaningful alt text site-wide	47 photos across the doctor directory; 9 photos on individual doctor profile pages
#5	Form fields rely on placeholder text instead of labels	Appointment scheduler (4 fields), patient portal sign-in (3 fields), contact form (2 fields)

2 Stabilize — 30 to 60 days 2 ITEMS

Close the high-risk findings — typically site-wide pattern fixes (design system color tokens, form-label patterns, focus-style refactor) that benefit from a single coordinated PR.

#3	Provider availability conveyed only by colored status dot	Find-a-doctor directory (1 page, 47 doctor cards)
#6	Focus indicators removed without replacement; new sticky-header obscure issue	Site-wide (every page) — focus outline removed in global CSS; sticky header obscures focused elements

3 Mature — 60 to 90 days 2 ITEMS

Address moderate and minor findings, plus the recommended-improvement bucket. This phase is where you move from "compliant" to "best-in-class" posture.

#7	Footer social-icon links fail target-size requirement (WCAG 2.2)	Site footer — 6 social icons on every page
#8	Insurance "Plan code" field has no example or help text	Billing & insurance form (1 page, 1 field — but high abandonment driver)

SECTION 1.6

Standards & regulations covered

Plain-English reference for every framework this report touches. We deliberately scope to the United States — these are the obligations you face if you serve US customers.

WCAG 2.2 (Levels A, AA, AAA)

GLOBAL · DE-FACTO US STANDARD

The Web Content Accessibility Guidelines from the W3C. The legal standard most US courts and agencies reference for digital accessibility. WCAG 2.2 (Oct 2023) added nine new criteria including Focus Not Obscured, Target Size, and Accessible Authentication.

WHAT IT MEANS FOR YOUR SITE

Every interactive element, form, page, and media asset must meet the level you target (AA is the typical bar).

ENFORCEMENT REALITY

Through ADA Title III litigation, DOJ guidance (Apr 2024), and state-level consumer protection.

ADA Title III

UNITED STATES — FEDERAL

The Americans with Disabilities Act prohibits discrimination by "places of public accommodation." DOJ and federal courts now interpret this to cover commercial websites and apps.

WHAT IT MEANS FOR YOUR SITE

Your website must be usable by people with disabilities — typically demonstrated via WCAG conformance. Private right of action with statutory damages.

ENFORCEMENT REALITY

Plaintiff-driven lawsuits (thousands filed per year in NY, CA, FL). Settlement ranges from $10k for small businesses to $1M+ for class actions.

Section 508

UNITED STATES — FEDERAL CONTRACTORS

Federal procurement standard requiring electronic/IT products to be accessible. Section 508 references WCAG 2.0 AA as its conformance benchmark.

WHAT IT MEANS FOR YOUR SITE

If your organization sells to or contracts with a US federal agency, your public-facing site and procured tools must conform.

ENFORCEMENT REALITY

Through procurement (lost contracts) and individual federal complaints.

CCPA / CPRA (California)

UNITED STATES — CALIFORNIA

The California Consumer Privacy Act (as amended by CPRA) gives California residents rights over their personal information: notice at collection, deletion, opt-out of sale, limit use of sensitive PI.

WHAT IT MEANS FOR YOUR SITE

You must display a clear "Do Not Sell or Share My Personal Information" link, a "Limit the Use of My Sensitive Personal Information" link if applicable, and a complete privacy policy.

ENFORCEMENT REALITY

California Privacy Protection Agency (CPPA) enforcement actions; private right of action for data breaches.

HIPAA — web component

UNITED STATES — FEDERAL (HEALTHCARE)

The Health Insurance Portability and Accountability Act protects PHI. The web-component subset covers transmission and disclosure — PHI in URLs, form security, browser autofill, session handling.

WHAT IT MEANS FOR YOUR SITE

If your site touches PHI (patient portals, appointment forms, billing), PHI must never appear in URLs, forms must use POST + HTTPS, and browser autofill of PHI fields must be disabled.

ENFORCEMENT REALITY

HHS Office for Civil Rights fines up to $1.9M per category per year; willful neglect violations can be criminal.

PCI-DSS — web component

GLOBAL — CARD-BRAND CONTRACTUAL

The Payment Card Industry Data Security Standard. Required by Visa, Mastercard, Amex, Discover, JCB for any organization that accepts cards.

WHAT IT MEANS FOR YOUR SITE

Checkout must be HTTPS only, payment forms must POST to HTTPS endpoints, and to qualify for the simplest validation level (SAQ-A) you should use a tokenization iframe so the card number never touches your origin.

ENFORCEMENT REALITY

Card-brand fines, increased transaction fees, loss of merchant processing privileges, mandatory forensic audits after a breach.

FERPA — web component

UNITED STATES — FEDERAL (EDUCATION)

The Family Educational Rights and Privacy Act protects student education records held by federally-funded institutions.

WHAT IT MEANS FOR YOUR SITE

If your site handles student records, student PII must never appear in URLs, all student-record pages must enforce HTTPS, and forms must use POST.

ENFORCEMENT REALITY

US Department of Education can withhold federal funding from institutions that violate FERPA.

SOC 2 (Trust Services Criteria)

GLOBAL — AUDITOR-ATTESTED

An AICPA framework for service organization controls. Buyers in regulated industries (finance, healthcare, federal) often require a SOC 2 Type II report before signing.

WHAT IT MEANS FOR YOUR SITE

The web-verifiable subset of SOC 2 — CC6.6 boundary protection, CC6.7 restricted transmission, CC6.8 malicious software prevention, CC9.1 risk mitigation — overlaps directly with the HTTP-security and privacy findings in this report.

ENFORCEMENT REALITY

Not a regulation — but a failed SOC 2 audit blocks enterprise deals and triggers re-audit costs.

PART 2 OF 2

Technical remediation

For engineering, design system owners, and SREs

Read this part to fix the findings. Every violation is listed exhaustively — every affected page, every CSS selector, every HTML snippet — alongside a before/after code template and a testing checklist your team can apply directly. The coverage summary is here too so you can verify what passed.

SECTION 2.1

How to use this guide

Each finding card below shows a single rule that failed, every occurrence across the audit, the underlying element HTML, a generic code-fix template, and a short testing checklist.

Reading a finding card

- **Rule ID** — stable identifier you can search in your bug tracker; matches axe-core's rule names or our internal compliance check IDs.
- **WCAG criteria** — for accessibility findings, the specific WCAG 2.2 success criterion. Cite this in your PR description.
- **Occurrences** — every page and every selector where the rule fired. Use this as a checklist.
- **Before / After code** — a template demonstrating the pattern, not a copy-paste for any one occurrence. Adapt to your component framework.
- **Verify with a rescan** — re-run this site in Plumb and confirm the rule reports 0 violations in the new report. Plumb is the verification loop — no need to leave the tool for axe, Lighthouse, or other scanners.

Suggested workflow

- Triage by severity bar color — critical first (red), then serious (orange).
- For findings that affect many elements, fix at the design-system primitive (e.g. one button color token, one focus-style rule) rather than per-occurrence.
- Use the page-by-page appendix in section 2.5 as a smoke-test list after each fix.

Total findings to address: **83** — 13 critical, 27 serious, 28 moderate, 15 minor.

SECTION 2.2

Coverage summary

Every check the scanner attempted, with pass/fail status. Use this as evidence of what was verified — not only what failed. **29** of **42** non-accessibility checks passed.

> **Modal coverage:** Plumb didn't detect any always-present dialog-shaped elements on the audited pages. If your app has modals (confirmation popups, "Add new" overlays, alert dialogs) that only render after a user interaction, they weren't audited — Plumb can't see modal HTML that doesn't exist in the DOM until clicked. For those, scan the URL with the modal already open, or wait for the per-page interaction-recipes feature.

Accessibility — WCAG 2.2 by principle

Zero findings in a principle is the strongest possible signal — every rule in that group ran and passed.

PRINCIPLE	WHAT IT COVERS	STATUS
1. Perceivable	Text alternatives, contrast, distinguishable content.	✗ 6 RULES FAILED (8 elements)
2. Operable	Keyboard access, navigation, target size, accessible auth.	✗ 4 RULES FAILED (5 elements)
3. Understandable	Readability, predictable behavior, input assistance.	✗ 2 RULES FAILED (3 elements)
4. Robust	Compatible with assistive technology, valid semantics.	✗ 4 RULES FAILED (4 elements)

Security, privacy, performance, industry compliance

Industry modules (HIPAA, PCI-DSS, FERPA) only emit findings on pages whose content triggers them. A passed status for those rows means either no relevant context was present or the checks succeeded.

HTTP security headers

4/6 passed

CHECK	STATUS	PAGES
Content-Security-Policy header	✗ FAILED	24 of 24
Strict-Transport-Security header	✗ FAILED	12 of 24
X-Frame-Options / CSP frame-ancestors	✓ PASSED	—
X-Content-Type-Options: nosniff	✓ PASSED	—
Referrer-Policy header	✓ PASSED	—
Permissions-Policy header	✓ PASSED	—

Privacy policy & CCPA disclosure

3/5 passed

CHECK	STATUS	PAGES
CCPA "Do Not Sell or Share" link	✗ FAILED	24 of 24
CPRA "Limit Sensitive PI Use" link	✗ FAILED	24 of 24
Privacy policy link present	✓ PASSED	—
Privacy policy link functional	✓ PASSED	—
Privacy policy URL returns 2xx HTML	✓ PASSED	—

Cookie consent & tracker inventory

1/3 passed

CHECK	STATUS	PAGES
Cookie banner when trackers present	✗ FAILED	1 of 24
Global Privacy Control awareness	✗ FAILED	1 of 24
Banner offers clear reject option	✓ PASSED	—

Core Web Vitals

5/7 passed

CHECK	STATUS	PAGES
Largest Contentful Paint ≤ 2.5s	✗ FAILED	3 of 24
Largest Contentful Paint ≤ 4s	✗ FAILED	1 of 24
Cumulative Layout Shift ≤ 0.25	✓ PASSED	—
Cumulative Layout Shift ≤ 0.1	✓ PASSED	—
Interaction to Next Paint ≤ 500ms	✓ PASSED	—
Interaction to Next Paint ≤ 200ms	✓ PASSED	—
Time to First Byte ≤ 1s	✓ PASSED	—

HIPAA web-component checks

4/6 passed

CHECK	STATUS	PAGES
No PHI identifiers in URLs	✗ FAILED	1 of 24
autocomplete=off on PHI fields	✗ FAILED	1 of 24
HTTPS enforced on PHI pages	✓ PASSED	—

CHECK	STATUS	PAGES
HSTS on HTTPS PHI pages	✓ PASSED	—
PHI forms use POST (not GET)	✓ PASSED	—
PHI form actions use HTTPS	✓ PASSED	—

PCI-DSS web-component checks

6/6 passed

CHECK	STATUS	PAGES
No card-number sequence in URLs	✓ PASSED	—
HTTPS enforced on checkout pages	✓ PASSED	—
Payment forms use POST	✓ PASSED	—
Payment form actions use HTTPS	✓ PASSED	—
Tokenization iframe (SAQ-A scope)	✓ PASSED	—
autocomplete=off on CVV input	✓ PASSED	—

FERPA web-component checks

5/5 passed

CHECK	STATUS	PAGES
No student PII in URLs	✓ PASSED	—
HTTPS on student-record pages	✓ PASSED	—
HSTS on student-record pages	✓ PASSED	—
Student-record forms use POST	✓ PASSED	—
Student-record form actions HTTPS	✓ PASSED	—

SOC 2 Trust Services evidence

1/4 passed

CHECK	STATUS	PAGES
CC6.8 — Malicious software prevention	✗ FAILED	24 of 24
CC9.1 — Risk mitigation	✗ FAILED	24 of 24
CC6.7 — Restricted transmission of data	✗ FAILED	1 of 24
CC6.6 — Boundary protection	✓ PASSED	—

SECTION 2.3

Accessibility findings

15 accessibility violations on your site, grouped into 14 rules. Every occurrence is listed exhaustively below — every page, every selector, every element. The before/after code blocks and testing checklist apply to all occurrences of the same rule.

1 additional finding on third-party redirect targets are listed at the end of this section as informational — they're on hosts you don't control (auth providers, payment processors) and cannot be fixed by your engineering team.

1. Elements must meet minimum color contrast ratio thresholds CRITICAL DESIGN SYSTEM

SEVERITY	CRITICAL	AFFECTS	2 pages, 2 elements
RULE ID	color-contrast	SOURCE	axe-core
WCAG	1.4.3 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Design system

SOLUTION

CODE FIX TEMPLATE

Update the color token at the design-system level rather than fixing each element. WCAG AA requires 4.5:1 for normal text, 3:1 for large text and UI components.

BEFORE

```
/* tokens.css */
:root {
  --color-primary: #6BA4D9;  /* 2.94:1 on white — FAILS AA */
}

.btn-primary {
  background: var(--color-primary);
  color: white;
}
```

AFTER

```
/* tokens.css */
:root {
  --color-primary: #2563EB;  /* 4.55:1 on white — passes AA */
}

.btn-primary {
  background: var(--color-primary);
  color: white;
}
```

DETECTION — ALL OCCURRENCES (2)

1. /

`.hero__cta`

```
<a class="hero__cta" href="/appointments">Book an appointment</a>
```

Element has insufficient color contrast of 2.94 (foreground color: #6BA4D9, background color: #ffffff, font size: 18.0pt). Expected contrast ratio of 4.5:1

2. /services

`.service-card__meta`

```
<span class="service-card__meta">Open today · 8am–6pm</span>
```

Insufficient contrast 3.71:1 — required 4.5:1 for normal text.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "color-contrast" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.

- Spot-check the highest-traffic CTAs visually against a white background.
- Confirm the new color still reads as "primary action" against your darker page sections (header, hero photos).

Reference: https://dequeuniversity.com/rules/axe/4.10/color-contrast

2. Images must have alternate text

CRITICAL CONTENT

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	image-alt	SOURCE	axe-core
WCAG	1.1.1 (A)	SECTION 508	502.3.1 / 501.1
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Every <img> needs either descriptive alt text (when the image conveys information) or alt="" (when the image is decorative and adjacent text identifies it).

BEFORE

```
<img src="/photos/dr-chen.jpg" class="doctor-card__photo">
<h3>Dr. Sarah Chen</h3>
<p>Cardiology</p>
```

AFTER

```
<!-- Decorative — name is in adjacent text -->
<img src="/photos/dr-chen.jpg" alt="" class="doctor-card__photo">
<h3>Dr. Sarah Chen</h3>
<p>Cardiology</p>

<!-- Informational variant -->
<img src="/diagram-heart-anatomy.png"
     alt="Cross-section diagram of the human heart with chambers labeled.">
```

DETECTION — ALL OCCURRENCES (1)

1. /find-a-doctor

`.doctor-card__photo > img`

```
<img src="/photos/dr-chen.jpg" class="doctor-card__photo">
```

Element does not have an alt attribute. The image will be announced as the file name to screen reader users.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "image-alt" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Walk the page with a screen reader (VoiceOver, NVDA, or JAWS) and confirm each image announces appropriately — informational images describe themselves, decorative alt="" images are skipped.

Reference: https://dequeuniversity.com/rules/axe/4.10/image-alt

3. Form elements must have labels

CRITICAL COMPONENT

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	`label`	SOURCE	axe-core
WCAG	1.3.1, 4.1.2 (A)	SECTION 508	502.3.1; 502.3.6 / 502.3.7
DOMAIN	Accessibility	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

Every <input> needs an associated <label>. Placeholder text disappears on focus and is not announced by all assistive technology — it is not a substitute.

BEFORE

```
<input type="text" name="dob" placeholder="Date
of birth">
```

AFTER

```
<label for="dob">Date of birth</label>
<input type="text"
       id="dob"
       name="dob"
       placeholder="MM/DD/YYYY"
       autocomplete="bday">
```

DETECTION — ALL OCCURRENCES (1)

1. /appointments

`input[name="dob"]`

```
<input type="text" name="dob" placeholder="Date of birth">
```

Form element does not have an associated label. Placeholder text is not a label and disappears on focus.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "label" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Click each label text and confirm focus jumps to the associated input.
- Screen-reader smoke test: focusing the input announces the label, not just "edit, blank".

Reference: https://dequeuniversity.com/rules/axe/4.10/label

4. Patient portal sign-in requires manual transcription of a multi-character code

CRITICAL AI COMPONENT

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	ai-auth-cognitive-test	SOURCE	Plumb AI
WCAG	3.3.8 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

WCAG 2.2 SC 3.3.8 Accessible Authentication (AA) prohibits requiring cognitive function tests (CAPTCHAs, transcription, puzzles) unless an alternative is offered. Add at least one alternative authentication path.

BEFORE

```
<form>
  <input name="email">
  <input type="password" name="password">
  <img class="captcha-image">
  <input name="captcha-answer">
  <button>Sign in</button>
</form>
```

AFTER

```
<form>
  <input name="email" autocomplete="email">
  <input type="password" name="password"
autocomplete="current-password">
  <button>Sign in</button>
</form>
<hr>
<!-- At least one alternative path -->
<form action="/auth/magic-link">
  <input name="email" autocomplete="email">
  <button>Email me a sign-in link</button>
</form>
<button class="passkey-btn">Sign in with a
passkey</button>
```

DETECTION — ALL OCCURRENCES (1)

1. /patient-portal

`.captcha-image + input`

```
<img class="captcha-image" alt="captcha"><input name="captcha-answer">
```

CAPTCHA-style image-text transcription is required to sign in. No alternative authentication method (passkey, OAuth, magic link). WCAG 2.2 explicitly prohibits this without an alternative.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "ai-auth-cognitive-test" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Verify a user can complete sign-in end-to-end without solving the CAPTCHA.
- Test the magic-link / passkey flow on a clean device with no saved credentials.

Reference: https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication-minimum

5. Links must have discernible text

SERIOUS CONTENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	link-name	SOURCE	axe-core
WCAG	2.4.4, 4.1.2 (A)	SECTION 508	502.3.1; 502.3.6 / 502.3.7
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Every link must have discernible text. Icon-only links need an aria-label or visually-hidden text.

BEFORE

```
<a href="/news/2026/cardiology-wing">
  <svg class="icon-arrow-right"></svg>
</a>
```

AFTER

```
<a href="/news/2026/cardiology-wing"
   aria-label="Read more: new cardiology wing">
  <svg class="icon-arrow-right" aria-
hidden="true"></svg>
</a>

<!-- Or with visible text + decorative icon -->
<a href="/news/2026/cardiology-wing">
  Read more <svg class="icon-arrow-right" aria-
hidden="true"></svg>
</a>
```

DETECTION — ALL OCCURRENCES (1)

1. /news

`.news-card a:has(svg)`

```
<a href="/news/2026/new-cardiology-wing"><svg class="icon-arrow-right"></svg></a>
```

Link only contains an SVG icon with no accessible name. Screen readers will announce "link" with no destination context.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "link-name" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Navigate by link list in a screen reader (VoiceOver: Ctrl+Option+U → Links). Every link should announce a meaningful destination.

Reference: https://dequeuniversity.com/rules/axe/4.10/link-name

6. Required ARIA attributes must be provided

SERIOUS COMPONENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	aria-required-attr	SOURCE	axe-core
WCAG	4.1.2 (A)	SECTION 508	502.3.6 / 502.3.7
DOMAIN	Accessibility	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

ARIA roles have required companion attributes. role="combobox" requires aria-expanded; role="slider" requires aria-valuenow; etc.

BEFORE

```
<div id="specialty-filter" role="combobox">All specialties</div>
```

AFTER

```
<div id="specialty-filter"
     role="combobox"
     aria-expanded="false"
     aria-controls="specialty-listbox"
     aria-haspopup="listbox"
     tabindex="0">All specialties</div>
```

DETECTION — ALL OCCURRENCES (1)

1. /find-a-doctor

`#specialty-filter[role="combobox"]`

```
<div id="specialty-filter" role="combobox">All specialties</div>
```

role="combobox" requires aria-expanded but it is not present.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "aria-required-attr" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Verify keyboard interaction: arrow keys open the list, escape closes it, enter selects.

Reference: https://dequeuniversity.com/rules/axe/4.10/aria-required-attr

7. Buttons must have discernible text

SERIOUS CONTENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	button-name	SOURCE	axe-core
WCAG	4.1.2 (A)	SECTION 508	502.3.6 / 502.3.7
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Every <button> needs accessible text — either inner text or aria-label.

BEFORE

```
<button class="password-toggle">
  <svg class="icon-eye"></svg>
</button>
```

AFTER

```
<button class="password-toggle"
        aria-label="Show password"
        aria-pressed="false">
  <svg class="icon-eye" aria-hidden="true"></svg>
</button>
```

DETECTION — ALL OCCURRENCES (1)

1. /patient-portal

`.password-toggle`

```
<button class="password-toggle"><svg class="icon-eye"></svg></button>
```

Button has no inner text and no aria-label. Screen reader users cannot tell what it does.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "button-name" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Screen-reader smoke test: the button announces its purpose, not just "button, button".

Reference: https://dequeuniversity.com/rules/axe/4.10/button-name

8. Focus indicators must be visible

SERIOUS DESIGN SYSTEM

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	`focus-visible`	SOURCE	axe-core
WCAG	2.4.7, 2.4.11 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Design system

SOLUTION

CODE FIX TEMPLATE

Never disable :focus styles without providing a clearly visible replacement. WCAG 2.2 also requires that focused elements not be obscured by sticky overlays (2.4.11).

BEFORE

```
a:focus, button:focus {
  outline: none;
}
```

AFTER

```
a:focus-visible, button:focus-visible {
  outline: 2px solid #2563EB;
  outline-offset: 2px;
  border-radius: 2px;
}

/* Fix sticky-header obscuring focused elements
(WCAG 2.4.11) */
html {
  scroll-padding-top: 80px; /* match your header
height */
}
```

DETECTION — ALL OCCURRENCES (1)

1. /

`a, button`

```
a:focus { outline: none; }
```

Default focus outline removed without a visible replacement. Keyboard-only users cannot see where focus is. Sticky header also obscures focused elements after scroll (WCAG 2.4.11 violation new in 2.2).

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "focus-visible" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Tab through the page with the keyboard — every focusable element should now show a visible focus ring.
- Scroll-tab past the sticky header and confirm the focused element scrolls into view above the header.

Reference: https://dequeuniversity.com/rules/axe/4.10/focus-visible

9. Image alt text is non-descriptive

SERIOUS AI CONTENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	ai-alt-text-quality	SOURCE	Plumb AI
WCAG	1.1.1 (A)	SECTION 508	502.3.1 / 501.1
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Alt text must convey the same information as the image. Generic strings like "image", "photo", or the filename are non-descriptive and fail WCAG 1.1.1.

BEFORE

```
<img src="/photos/team.jpg" alt="image">
<img src="/icons/search.svg" alt="search.svg">
```

AFTER

```
<img src="/photos/team.jpg"
     alt="The Cascade Valley Health executive
team in front of the main hospital building.">

<!-- For icon buttons, label the button, not the
icon. -->
<button aria-label="Search">
  <img src="/icons/search.svg" alt="">
</button>
```

DETECTION — ALL OCCURRENCES (1)

1. /about

`.about-hero img`

```
<img src="/photos/team.jpg" alt="image">
```

Alt text "image" provides no information. Screen reader announces "image, image" — the word twice.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "ai-alt-text-quality" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Read each new alt aloud — does it convey what the image actually shows?
- For text-bearing images, confirm the visible text is transcribed verbatim into the alt.

Reference: https://www.w3.org/WAI/WCAG22/Understanding/non-text-content

10. Generic "Read more" link text used 14 times on the same page

SERIOUS AI CONTENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	ai-link-text-vague	SOURCE	Plumb AI
WCAG	2.4.4 (A)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Out-of-context navigation (screen-reader rotors, tab key) presents links without surrounding text. Each link must communicate its destination on its own.

BEFORE

```
<!-- 14 identical "Read more" links on the page -->
<a href="/news/cardiology-wing" class="read-more">Read more</a>
<a href="/news/new-pediatrics-lead" class="read-more">Read more</a>
```

AFTER

```
<a href="/news/cardiology-wing"
   class="read-more"
   aria-label="Read more about the new cardiology wing">Read more</a>

<a href="/news/new-pediatrics-lead"
   class="read-more"
   aria-label="Read more about our new pediatrics lead">Read more</a>

<!-- Better: include the article title in the link text itself -->
<a href="/news/cardiology-wing" class="news-card-link">
  New cardiology wing opens
</a>
```

DETECTION — ALL OCCURRENCES (1)

1. /news

`.news-card a.read-more`

```
<a href="/news/2026/cardiology-wing" class="read-more">Read more</a>
```

Screen reader users navigating by link list (a common pattern) hear "Read more, link" 14 times in a row with no way to distinguish destinations.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "ai-link-text-vague" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.

- Activate the screen-reader link-rotor and confirm each previously-identical link now announces uniquely.

Reference: https://www.w3.org/WAI/WCAG22/Understanding/link-purpose-in-context

11. Heading levels should only increase by one

MODERATE COMPONENT

SEVERITY	MODERATE	AFFECTS	**1** page, **1** element
RULE ID	`heading-order`	SOURCE	axe-core
WCAG	1.3.1 (A)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

Heading levels must not skip. After an h2, the next heading is h2 or h3 — never h4 directly.

BEFORE

```
<h2>Cardiology services</h2>
<h4>Conditions we treat</h4>
```

AFTER

```
<h2>Cardiology services</h2>
<h3>Conditions we treat</h3>
```

DETECTION — ALL OCCURRENCES (1)

1. /services/cardiology

`main h4`

```
<h4>Conditions we treat</h4>
```

Heading order skips from h2 to h4, breaking document outline.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "heading-order" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- View the page outline with a screen reader heading-list (VoiceOver: Ctrl+Option+U → Headings). The hierarchy should now make sense end-to-end.

Reference: https://dequeuniversity.com/rules/axe/4.10/heading-order

12. Touch targets must be at least 24×24 CSS pixels

MODERATE DESIGN SYSTEM

SEVERITY	MODERATE	AFFECTS	1 page, 1 element
RULE ID	`target-size`	SOURCE	axe-core
WCAG	2.5.8 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Design system

SOLUTION

CODE FIX TEMPLATE

WCAG 2.2 added Target Size (Minimum) at AA: each touch target must be at least 24×24 CSS pixels, OR be spaced at least 24px from adjacent targets. The visible icon size can stay smaller — only the tappable area must grow.

BEFORE

```
.social-icon-link {
  width: 18px; height: 18px;
  margin-right: 4px;
}
```

AFTER

```
.social-icon-link {
  display: inline-flex;
  align-items: center;
  justify-content: center;
  width: 24px; height: 24px;  /* satisfies 2.5.8
*/
  margin-right: 8px;
}
.social-icon-link svg {
  width: 18px; height: 18px;  /* visual size
unchanged */
}
```

DETECTION — ALL OCCURRENCES (1)

1. /

`.social-icon-link`

```
<a class="social-icon-link" href="/twitter"><svg></svg></a>
```

Footer social icons are 18×18 with 4px spacing. WCAG 2.2 AA requires 24×24 minimum unless adjacent targets are spaced 24px apart.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "target-size" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Try the page on a touch device with one-finger input — missing taps on adjacent icons should drop sharply.

Reference: https://dequeuniversity.com/rules/axe/4.10/target-size

13. Provider availability conveyed only by color

MODERATE AI CONTENT

SEVERITY	MODERATE	AFFECTS	1 page, 1 element
RULE ID	ai-color-only-info	SOURCE	Plumb AI
WCAG	1.4.1 (A)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

Information must not be conveyed by color alone. Pair every color signal with text, icon shape, or pattern.

BEFORE

```
<span class="availability-dot availability-dot--green"></span>
```

AFTER

```
<span class="availability-status availability-status--accepting">
  <span class="availability-dot availability-dot--green"
        aria-hidden="true"></span>
  Accepting new patients
</span>
```

DETECTION — ALL OCCURRENCES (1)

1. /find-a-doctor

`.availability-dot`

```
<span class="availability-dot availability-dot--green"></span>
```

A green dot means "accepting new patients", a gray dot means "not accepting". Color-blind users (especially deuteranopia) cannot distinguish these reliably; screen reader users hear nothing.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "ai-color-only-info" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Simulate color-blindness (browser DevTools → Rendering → Emulate vision deficiencies). Every status must still be distinguishable.
- Screen-reader smoke test: announcement now includes the text status, not just the dot.

Reference: https://www.w3.org/WAI/WCAG22/Understanding/use-of-color

14. Insurance form requires patients to know obscure plan codes

MODERATE AI COMPONENT

SEVERITY	MODERATE	AFFECTS	1 page, 1 element
RULE ID	ai-cognitive-form-instructions	SOURCE	Plumb AI
WCAG	3.3.2, 3.3.3 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

WCAG 3.3.2 requires labels and instructions for inputs that need them. Add an example, an autocomplete attribute, and a help link or modal where the value is non-obvious.

BEFORE

```
<label for="planCode">Plan code</label>
<input id="planCode" name="planCode">
```

AFTER

```
<label for="planCode">Plan code</label>
<input id="planCode"
       name="planCode"
       placeholder="Example: BCBS-PPO-2024"
       aria-describedby="planCode-help">
<small id="planCode-help">
  Find this on your insurance card.
  <a href="#" data-modal="planCode-help">Show me
where</a>
</small>
```

DETECTION — ALL OCCURRENCES (1)

1. /billing

`input[name="planCode"]`

```
<label for="planCode">Plan code <input id="planCode" name="planCode"></label>
```

No example, no help link, no autocomplete from common providers. Patients have to guess at internal Cascade Valley plan-code format (e.g. "BCBS-PPO-2024").

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "ai-cognitive-form-instructions" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- User-test with a non-engineer: can they fill the field on first try without external help?

Reference: https://www.w3.org/WAI/WCAG22/Understanding/labels-or-instructions

Informational — third-party redirect targets

These findings are on hosts your scan crossed during authentication or external embeds. Your team cannot fix them; they are listed for completeness. Examples: Azure AD login pages, Stripe iframes, Google OAuth consent screens.

1. Elements must meet minimum color contrast ratio thresholds SERIOUS INFORMATIONAL

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	color-contrast	SOURCE	axe-core
WCAG	1.4.3 (AA)	SECTION 508	502.3.1
DOMAIN	Accessibility	FIX SCOPE	Design system

SOLUTION

CODE FIX TEMPLATE

Update the color token at the design-system level rather than fixing each element. WCAG AA requires 4.5:1 for normal text, 3:1 for large text and UI components.

BEFORE

```
/* tokens.css */
:root {
  --color-primary: #6BA4D9;  /* 2.94:1 on white — FAILS AA */
}

.btn-primary {
  background: var(--color-primary);
  color: white;
}
```

AFTER

```
/* tokens.css */
:root {
  --color-primary: #2563EB;  /* 4.55:1 on white — passes AA */
}

.btn-primary {
  background: var(--color-primary);
  color: white;
}
```

DETECTION — ALL OCCURRENCES (1)

1. /login

`.auth0-lock-submit`

```
<button class="auth0-lock-submit" data-action-text="Log in">Log in</button>
```

Auth0 default theme submit button has contrast 3.91:1 — below 4.5:1 minimum. Auth0 controls this; if visual brand parity matters, configure custom universal-login HTML/CSS in the Auth0 dashboard.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "color-contrast" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Spot-check the highest-traffic CTAs visually against a white background.
- Confirm the new color still reads as "primary action" against your darker page sections (header, hero photos).

Reference: https://dequeuniversity.com/rules/axe/4.10/color-contrast

SECTION 2.4

Other compliance findings

Findings outside WCAG: HTTP security headers, privacy & CCPA, cookie consent, Core Web Vitals, HIPAA, PCI-DSS, FERPA, and SOC 2 evidence. Each finding includes the same exhaustive occurrence list and code-fix template as the accessibility section.

1 additional finding on third-party redirect targets are listed at the end of this section as informational.

HTTP security headers

1. Missing Content-Security-Policy header

CRITICAL INFRA CONFIG

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	security-missing-csp	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Security	FIX SCOPE	Infra config

SOLUTION

CODE FIX TEMPLATE

Set a Content-Security-Policy header. Start with a restrictive default-src and allowlist only the origins your site actually needs.

BEFORE

```
# No Content-Security-Policy header in responses
```

AFTER

```
# Express middleware example
app.use((req, res, next) => {
  res.setHeader(
    'Content-Security-Policy',
    "default-src 'self'; " +
    "script-src 'self' 'nonce-{nonce}'
https://cdn.example.com; " +
    "style-src 'self' 'unsafe-inline'; " +
    "img-src 'self' data: https:; " +
    "connect-src 'self' https://api.example.com;
" +
    "frame-ancestors 'none';"
  );
  next();
});
```

DETECTION — ALL OCCURRENCES (1)

1. /

`response-headers`

No Content-Security-Policy header. The browser applies no script-source, frame-source, or other policy restrictions — XSS, click-jacking, and tracker injection are unmitigated. Critical for a healthcare site rendering patient-facing forms.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "security-missing-csp" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Watch the browser console as you walk the site — CSP-violation reports should be empty. Add any legitimate origin you missed to the policy allowlist.

Reference: https://developer.mozilla.org/docs/Web/HTTP/CSP

2. Strict-Transport-Security max-age too short

SERIOUS INFRA CONFIG

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	security-missing-hsts	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Security	FIX SCOPE	Infra config

SOLUTION

CODE FIX TEMPLATE

Set Strict-Transport-Security with a max-age of at least 6 months and includeSubDomains. Add preload once you are confident every subdomain is HTTPS-only.

BEFORE

```
# Header absent OR max-age too short
Strict-Transport-Security: max-age=86400
```

AFTER

```
Strict-Transport-Security: max-age=31536000;
includeSubDomains; preload
```

DETECTION — ALL OCCURRENCES (1)

1. /patient-portal

`response-headers`

HSTS max-age=86400 (1 day) — Mozilla baseline is 6 months (15552000). On a HIPAA-handling site, returning patients should never be downgradeable to HTTP. Set max-age=31536000; includeSubDomains; preload.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "security-missing-hsts" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.

Reference: https://developer.mozilla.org/docs/Web/HTTP/Headers/Strict-Transport-Security

Privacy policy & CCPA disclosure

1. Missing CCPA / CPRA "Do Not Sell or Share" link

SERIOUS CONTENT

SEVERITY	SERIOUS	AFFECTS	1 page, 1 element
RULE ID	`privacy-missing-do-not-sell-link`	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Privacy	FIX SCOPE	Content

SOLUTION

CODE FIX TEMPLATE

CCPA / CPRA requires a clear and conspicuous "Do Not Sell or Share My Personal Information" link on the homepage and any page that collects personal information from California residents.

BEFORE

```
<!-- Footer with no CCPA link -->
<footer>
  <a href="/privacy">Privacy Policy</a>
</footer>
```

AFTER

```
<footer>
  <a href="/privacy">Privacy Policy</a>
  <a href="/do-not-sell">Do Not Sell or Share My Personal Information</a>
  <a href="/limit-use">Limit the Use of My Sensitive Personal Information</a>
</footer>
```

DETECTION — ALL OCCURRENCES (1)

1. /

`body`

CPRA requires a clear and conspicuous "Do Not Sell or Share My Personal Information" link on the homepage and any page that collects personal information from California residents. Not detected. California patients have a private right of action under CPRA for data-breach scenarios.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "privacy-missing-do-not-sell-link" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Manually click the new link from a few entry pages and confirm the destination presents a working opt-out mechanism (form, toggle, or contact path).

Reference: https://oag.ca.gov/privacy/ccpa

Cookie consent & tracker inventory

1. Trackers loaded with no visible cookie / privacy banner

CRITICAL COMPONENT

SEVERITY	CRITICAL	AFFECTS	**1** page, **1** element
RULE ID	`cookie-consent-missing-banner-with-trackers`	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Cookie consent	FIX SCOPE	Component

SOLUTION

HOW TO FIX

Trackers loaded with no visible cookie / privacy banner.

Approach: Inspect each occurrence listed below — the *per-element notes* describe exactly what failed (expected vs actual, missing attributes, etc.). Apply the corresponding fix to each affected element, prioritizing the design-system / component-library level so a single change cascades to every occurrence. Authoritative remediation guidance for this specific rule is at the reference link at the bottom of this card.

DETECTION — ALL OCCURRENCES (1)

1. /

`body`

The page loads Google Analytics (analytics), Meta Pixel (advertising), Hotjar (session-replay), and Microsoft Clarity (analytics) but no consent banner was detected. CCPA / CPRA requires notice at collection — exposes the operator to enforcement action and private right-of-action lawsuits.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "cookie-consent-missing-banner-with-trackers" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.

Reference: https://oag.ca.gov/privacy/ccpa

Core Web Vitals

1. Largest Contentful Paint is 4.82s (poor: >4s)

SERIOUS COMPONENT

SEVERITY	SERIOUS	AFFECTS	**1** page, **1** element
RULE ID	`perf-lcp-poor`	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Performance	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

LCP > 4s is in Google's "poor" band. The hero image is typically the LCP element. Preload it with fetchpriority="high", defer non-critical JS, and serve appropriately sized images.

BEFORE

```
<img src="/hero-2400x1600.jpg" class="hero-
image">
<script src="/analytics.js"></script>
<script src="/social-widgets.js"></script>
```

AFTER

```
<!-- In <head> -->
<link rel="preload" as="image"
      href="/hero-1200x800.webp"
      fetchpriority="high"
      imagesrcset="/hero-800x533.webp 800w,
/hero-1200x800.webp 1200w"
      imagesizes="100vw">

<!-- In <body> -->
<img src="/hero-1200x800.webp"
     fetchpriority="high"
     loading="eager"
     decoding="async"
     class="hero-image">

<script src="/analytics.js" defer></script>
<script src="/social-widgets.js" defer></script>
```

DETECTION — ALL OCCURRENCES (1)

1. /find-a-doctor

`body`

LCP measures when the largest visible element finished painting. At 4.82s this page is in Google's "poor" band — a documented ranking-signal demotion. Hero physician headshots are 1.2 MB each and not preloaded; defer the analytics bundle and add fetchpriority="high" to the hero image.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "perf-lcp-poor" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.

- After the rescan passes the synthetic check, watch real-user field data in your RUM for 14–28 days — synthetic LCP and field LCP can diverge under real-world network conditions.

Reference: https://web.dev/articles/lcp

HIPAA web-component checks

1. PHI identifier in URL query string

CRITICAL BACKEND CODE

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	hipaa-phi-in-url	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	HIPAA	FIX SCOPE	Backend code

SOLUTION

CODE FIX TEMPLATE

PHI must never appear in URLs — URLs are written to access logs, browser history, third-party referrers, and CDN caches, all of which are outside HIPAA-safe scope. Pass the identifier in the request body and resolve from the server-side session.

BEFORE

```
<!-- URL pattern: /portal/dashboard?
patientid=A4729183 -->
<a href="/portal/dashboard?
patientid=A4729183">Open my chart</a>
```

AFTER

```
<!-- Server stores patient id in session; client
request is opaque -->
<a href="/portal/dashboard">Open my chart</a>

<!-- Server route -->
app.get('/portal/dashboard', (req, res) => {
  const patientId = req.session.patientId; //
from authenticated session
  // ... render ...
});
```

DETECTION — ALL OCCURRENCES (1)

1. /patient-portal

body

The patient portal session-resume flow passes the patient MRN in the URL (?patientid=A4729183). URLs are written to server access logs, browser history, third-party referrer headers, and CDN caches — none of which have a Business Associate Agreement. Switch to POST with the value in the request body and look it up from the authenticated session server-side.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "hipaa-phi-in-url" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Walk every patient-portal flow with the browser address bar visible and confirm no PHI ever appears in the URL.
- Audit your server access logs, CDN edge logs, and third-party scripts (RUM, session replay) for any inadvertent PHI capture from older URLs — purge where found.

Reference: https://www.hhs.gov/hipaa/for-professionals/security/

2. PHI-sensitive fields allow browser autocomplete

MODERATE COMPONENT

SEVERITY	MODERATE	AFFECTS	1 page, 1 element
RULE ID	`hipaa-phi-field-autocomplete`	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	HIPAA	FIX SCOPE	Component

SOLUTION

CODE FIX TEMPLATE

PHI-bearing form fields should set autocomplete="off" to prevent the browser from caching the value where another user of the same device could autofill it. This is a documented HIPAA review gap.

BEFORE

```
<label for="memberId">Member ID</label>
<input id="memberId" name="memberId">
```

AFTER

```
<label for="memberId">Member ID</label>
<input id="memberId"
       name="memberId"
       autocomplete="off"
       inputmode="text">
```

DETECTION — ALL OCCURRENCES (1)

1. /billing

`body`

The insurance form's "Member ID" and "Date of Birth" inputs don't set autocomplete="off". Browsers cache values to disk where another user of the same machine could autofill them — a documented HIPAA review gap.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "hipaa-phi-field-autocomplete" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Manual: fill a form once, then on a fresh session see whether the browser offers to autofill the field. It should not.

Reference: https://www.hhs.gov/hipaa/for-professionals/security/

SOC 2 Trust Services evidence

1. Trust Services Criterion CC6.7 — restricted transmission gap

CRITICAL INFRA CONFIG

SEVERITY	CRITICAL	AFFECTS	1 page, 1 element
RULE ID	soc2-cc6.7-gap	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	SOC 2	FIX SCOPE	Infra config

SOLUTION

CODE FIX TEMPLATE

CC6.7 (restricted transmission of data) is a composite criterion — it rolls up the underlying HTTPS/HSTS/TLS findings. Close those (security-missing-hsts, hipaa-missing-hsts) and the CC6.7 gap closes with them.

BEFORE

```
# Underlying findings:
# - security-missing-hsts
# - hipaa-missing-hsts on /patient-portal
```

AFTER

```
# Resolution:
# 1. Add HSTS with max-age >= 6 months
# 2. Force HTTPS via 301 redirect on all HTTP requests
# 3. Audit TLS config — Mozilla Intermediate or stricter
# 4. Document the change in your SOC 2 system description
```

DETECTION — ALL OCCURRENCES (1)

1. /patient-portal

`body`

CC6.7 (restricted transmission of data) is impaired by underlying findings security-missing-hsts and hipaa-missing-hsts on this page. Address those root-cause findings to close the control gap. This audit covers only the web-verifiable subset of SOC 2 — your access reviews, change management, and incident response are out of scope.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "soc2-cc6.7-gap" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Once the rescan confirms the underlying HSTS findings are closed, attach the before/after Plumb reports to your SOC 2 system description as auditor evidence.

Reference: https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

Informational — third-party redirect targets

Compliance findings on hosts your scan crossed during authentication or external embeds (Azure AD, Stripe, Google sign-in, etc.). Your team cannot fix CSP or other headers on these hosts; the findings are listed for completeness and may be useful when evaluating third-party vendors.

1. Missing Content-Security-Policy header

CRITICAL INFORMATIONAL

SEVERITY	CRITICAL	AFFECTS	2 pages, 2 elements
RULE ID	`security-missing-csp`	SOURCE	Compliance module
WCAG	—	SECTION 508	—
DOMAIN	Security	FIX SCOPE	Infra config

SOLUTION

CODE FIX TEMPLATE

Set a Content-Security-Policy header. Start with a restrictive default-src and allowlist only the origins your site actually needs.

BEFORE

```
# No Content-Security-Policy header in responses
```

AFTER

```
# Express middleware example
app.use((req, res, next) => {
  res.setHeader(
    'Content-Security-Policy',
    "default-src 'self'; " +
    "script-src 'self' 'nonce-{nonce}'
https://cdn.example.com; " +
    "style-src 'self' 'unsafe-inline'; " +
    "img-src 'self' data: https:; " +
    "connect-src 'self' https://api.example.com;
" +
    "frame-ancestors 'none';"
  );
  next();
});
```

DETECTION — ALL OCCURRENCES (2)

1 occurrence on `cascadevalleyhealth-tenant.us.auth0.com`

1. /login

`response-headers`

No Content-Security-Policy header on the Auth0 hosted login page. This is on Auth0's infrastructure, not yours — listed for vendor risk awareness, but not a fix for your engineering team. If CSP compliance on the auth surface is contractually required, request the Auth0 Enterprise Custom Domain or escalate to Auth0 support.

1 occurrence on `js.stripe.com`

2. /v3/elements-inner-payment-element-abc123.html

`response-headers`

No Content-Security-Policy header on the Stripe Elements iframe inner. Stripe controls this infrastructure; PCI compliance posture is covered by Stripe's SAQ-D-on-behalf-of-merchant. No engineering action required.

VERIFICATION

HOW TO VERIFY — RESCAN WITH PLUMB

- Re-run this site in Plumb once the fix has shipped — from the dashboard click "Rescan", or paste the URL back at /scan. The new report's Coverage Summary should show "security-missing-csp" reporting 0 violations.
- Open the new report and confirm the previously-affected pages now show a "✓ Clean" badge in the Page-by-page appendix (section 2.5) for this rule.
- Watch the browser console as you walk the site — CSP-violation reports should be empty. Add any legitimate origin you missed to the policy allowlist.

Reference: https://developer.mozilla.org/docs/Web/HTTP/CSP

SECTION 2.5

Page-by-page appendix

Every page audited, with the full list of failing rules and per-page element counts. Useful as a smoke-test checklist after fixes ship — rescan and confirm each previously-flagged page now reports "Clean."

Home — Cascade Valley Health

6 issues

https://cascadevalleyhealth.example/

- CRITICAL `color-contrast` — 1 element
- CRITICAL `security-missing-csp` — 1 element
- CRITICAL `cookie-consent-missing-banner-with-trackers` — 1 element
- SERIOUS `focus-visible` — 1 element
- SERIOUS `privacy-missing-do-not-sell-link` — 1 element
- MODERATE `target-size` — 1 element

Find a Doctor

4 issues

https://cascadevalleyhealth.example/find-a-doctor

- CRITICAL `image-alt` — 1 element
- SERIOUS `aria-required-attr` — 1 element
- SERIOUS `perf-lcp-poor` — 1 element
- MODERATE `ai-color-only-info` — 1 element

Services & Specialties

1 issue

https://cascadevalleyhealth.example/services

- SERIOUS `color-contrast` — 1 element

Cardiology

1 issue

https://cascadevalleyhealth.example/services/cardiology

- MODERATE `heading-order` — 1 element

Patient Portal Login

5 issues

https://cascadevalleyhealth.example/patient-portal

- CRITICAL `ai-auth-cognitive-test` — 1 element
- CRITICAL `hipaa-phi-in-url` — 1 element
- CRITICAL `soc2-cc6.7-gap` — 1 element
- SERIOUS `button-name` — 1 element
- SERIOUS `security-missing-hsts` — 1 element

Schedule an Appointment

1 issue

https://cascadevalleyhealth.example/appointments

- CRITICAL `label` — 1 element

Billing & Insurance

2 issues

https://cascadevalleyhealth.example/billing

- MODERATE ai-cognitive-form-instructions — 1 element
- MODERATE hipaa-phi-field-autocomplete — 1 element

Contact Us

✓ Clean

https://cascadevalleyhealth.example/contact

No findings on this page.

About Us

1 issue

https://cascadevalleyhealth.example/about

- SERIOUS ai-alt-text-quality — 1 element

News & Press

2 issues

https://cascadevalleyhealth.example/news

- SERIOUS link-name — 1 element
- SERIOUS ai-link-text-vague — 1 element