ClinicOps

FREE CHECKLIST

HIPAA Website Checklist

Find where your website can leak patient information (forms, trackers, chat, scheduling, email) and close it, with a risk score for every page.

Patients type health information into your website every day: appointment requests, contact forms, intake, chat. This checklist finds every place that information goes, checks that each vendor who touches it has signed a business associate agreement, and keeps advertising and analytics trackers away from it.

Jun 20, 2024
a federal court vacated one part of HHS's tracking guidance, and only that part
AHA v. Becerra, N.D. Tex.

60 days
the outer limit to notify patients after a breach is discovered
45 CFR 164.404(b)

500+
residents of one state affected by a breach: notify the media there too
45 CFR 164.406

What the rules say now (Nov 2026)

Rule	What it means for your website	Source
Health information a patient gives you is IIHI	A form entry that relates to someone's health or care and identifies them (name, phone, email) is individually identifiable health information once your practice receives it.	45 CFR 160.103
Vendors who handle it need a BAA	Anyone who creates, receives, maintains or transmits that information for you (form tool, scheduler, chat, host that stores submissions) is a business associate and must sign an agreement first.	45 CFR 160.103; 164.502(e); 164.504(e)
Protect it in transit	Guard electronic PHI sent over a network; encryption is an addressable specification. In practice: HTTPS everywhere and no plain email of form contents.	45 CFR 164.312(e)
Tracking technologies	HHS OCR's tracking bulletin (Dec 2022, revised Mar 18, 2024) still stands except one part: on Jun 20, 2024 a federal court vacated the part treating an IP address plus a visit to an unauthenticated public page about conditions or providers as protected. The court said the vacatur does not limit the rest of the document.	AHA v. Becerra, No. 4:23-cv-01110-P (N.D. Tex. Jun 20, 2024)
Breach clock	Notify affected patients without unreasonable delay and no later than 60 calendar days after discovery. Tell HHS at the same time for 500 or more people; within 60 days of year end for fewer.	45 CFR 164.404(b); 164.408

The FTC Health Breach Notification Rule does not apply to HIPAA covered entities (16 CFR 318.1); state privacy laws can add to HIPAA. This is operations guidance, not legal advice: have your privacy officer or counsel confirm decisions about your own site.

Step 1: inventory every page that matters (20 minutes)

1. List your pages with a form, a login, a booking widget or a chat box, plus your home page and your most visited condition or service pages.
2. Find the third-party scripts on each: ask your web vendor for a list of every tag and pixel, open your tag manager, or open the page in a browser's developer tools (Network tab) and note every outside domain that loads.
3. Follow each form: submit a test entry with fake details and see where it lands (the form vendor, an email inbox, your EHR) and who can read it.
4. Check each vendor for a signed business associate agreement, and file the copy.

Page or element	Collects health info or login?	Third-party scripts found	Where submissions go	BAA signed?
Home page				
Condition or service pages				
Appointment request form				
Contact form				
Online scheduling widget				
Intake or new patient forms				
Patient portal login				
Chat box				
Reviews or testimonials widget				
Careers or other form				

Step 2: check each element

FORMS

- [ ] **Every page loads over HTTPS and every form posts over HTTPS.**
  Transmission security, 45 CFR 164.312(e).
- [ ] **Form submissions are stored by a vendor that has signed a BAA, or go straight into your EHR or portal, not into a plain email inbox.**
  A notification email that contains the patient's details is PHI in transit.
- [ ] **Each form asks only for what the front desk needs to call back or book: no free-text symptom box unless a clinician needs it.**
  Our standard: less collected, less to protect.
- [ ] **The autoresponder says "we received your request" and nothing about the reason for the visit.**
  Least necessary in anything sent outside your systems.

TRACKERS AND ANALYTICS

- [ ] **No advertising pixel or analytics tag runs on pages where patients log in, book, or type health information, unless the vendor has signed a BAA.**
  The vacated part of the guidance covered only public pages; logged-in pages and what patients type are not cleared by the ruling.
- [ ] **The tag manager lists every tag, who added it and why. Tags nobody can explain are removed.**
  Most leaks come from tags added years ago by someone who has left.
- [ ] **Session recording and heatmap tools are off on every form and portal page.**
  They can capture what a patient types.

CHAT, SCHEDULING, EMAIL AND ACCESS

- [ ] **Chat: the vendor signs a BAA, or the chat tells patients not to share health details and routes them to the phone or portal.**
  Transcripts are stored by the vendor.
- [ ] **Scheduling: the widget vendor signs a BAA, and confirmation emails or texts give a time and place, not a reason.**
  45 CFR 164.502(e).
- [ ] **Your web agency or freelancer can read form submissions only under a BAA; otherwise remove that access.**
  Admin access to stored submissions is access to PHI.
- [ ] **Logins to the site, the form tool and the tag manager use multi-factor sign-in, and leavers are removed the day they leave.**
  Access control, 45 CFR 164.312(a).
- [ ] **Review replies never confirm that the reviewer is a patient or mention their care.**
  Our standard: thank them and invite them to call.

Step 3: score the risk of each page

Add the points that apply to each page (a ClinicOps scoring method, not a regulator's formula). The worked example scores three pages of an illustrative site.

If this is true for the page	Points
Patients type health information here, or log in	3
A third-party advertising or analytics script runs here	3
A vendor that touches the submissions has no signed BAA	3
Submissions arrive by plain email	2
Session recording or heatmaps run here	2
Nobody can say who added each script	1

Page	Worked example: points	Example score	Your score
Appointment request form	Health info 3 + pixel 3 + plain email 2	8	
Patient portal login	Login 3 + analytics 3	6	
Blog post on a condition	Analytics 3 (public page, nothing typed)	3	
Your page:			
Your page:			

0 to 3	Low	Keep the inventory current; recheck after every site change.
4 to 6	Fix this month	Remove the script or get the BAA; move form delivery off email.
7 and up	Fix this week	Take the tracker off the page today. If PHI may already have gone to a vendor without a BAA, call your privacy officer: the breach clock may be running.

The size of your exposure

A ClinicOps calculation from your own numbers: how many patients a year use pages that scored 7 or more.

Line	How to get it	Worked example	Yours
A. Form submissions a month on pages scoring 7+	Your form tool's or inbox count	60	
B. Portal logins a month on pages scoring 7+	Your portal report	0	
C. Patient interactions exposed a year	(A + B) x 12	720	
D. Over 500?	If yes, a reportable breach would also mean telling HHS at the same time and, for 500+ in one state, the media	Yes	

When it goes wrong

When this happens	Do this
You find an advertising pixel on the booking or intake page	Remove it today, note when it was added, and ask your privacy officer whether submissions reached the vendor: that decides whether a breach assessment starts.
Form submissions have been going to a personal or free email inbox	Point the form to the BAA-covered tool or your EHR today, delete the copies in the inbox, and tell your privacy officer.
A vendor will not sign a BAA	Stop sending it PHI: remove the tool from pages where patients type health information, or replace it with one that signs.
You suspect a breach	Your privacy officer runs the breach risk assessment. If notice is needed, patients hear within 60 calendar days of discovery at the latest (45 CFR 164.404(b)).
A patient posts health details in a public review	Do not confirm or add to it. Reply with a general thank-you and an invitation to call.
Your web agency adds a new plugin	Agree in writing that nothing goes on form, booking or portal pages without your sign-off; re-run Step 1 after every change. Unpublish old landing pages with forms.

Next steps: run Step 1 this week, fix every page that scores 7 or more before anything else, then file the BAAs in one folder with a renewal check each year. The full guide, with the court ruling explained, is on clinicops.us.

Sources

Every figure and rule here was checked against the original source on Nov 18, 2026. Rules and figures change: confirm anything time-sensitive on the source page.

1. American Hospital Association v. Becerra, No. 4:23-cv-01110-P, memorandum opinion and order (N.D. Tex.), Proscribed Combination declared unlawful and vacated; footnote 8 on the rest of the guidance (Jun 20, 2024). aha.org/system/files/media/file/2024/06/opinion-order-in-aha-et-al-v-xavier-be

2. HHS OCR, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (revised Mar 18, 2024). hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.h

3. 45 CFR 160.103 (individually identifiable health information; business associate) (eCFR, current). ecfr.gov/current/title-45/section-160.103

4. 45 CFR 164.502(e), 164.504(e) business associate contracts; 164.312(a), (e) access control and transmission security (eCFR, current). ecfr.gov/current/title-45/section-164.312

5. 45 CFR 164.404(b), 164.406, 164.408 breach notification to individuals, media and HHS (eCFR, current). ecfr.gov/current/title-45/section-164.404

6. 16 CFR 318.1, FTC Health Breach Notification Rule, scope (eCFR, current). ecfr.gov/current/title-16/section-318.1

Where this checklist stops

The checklist shows you where the leaks are. Here is what it cannot do on its own:

- **It cannot see your code. Scripts are added by plugins, agencies and tag managers long after anyone reads a checklist.**
- **It cannot sign BAAs or move your forms. The fixes need someone with access to the site and the vendors.**
- **It cannot tell you whether a past leak is a reportable breach. That is your privacy officer's or counsel's call.**

Website plus AI Visibility: a fast, HIPAA-aware website on your own accounts, set up so Google and AI assistants can find and recommend you.

Book the free 20-minute Chaos Audit >

It is a diagnostic call, not a sales call: we walk back the last thing that slipped, put an hours or dollar figure on it, and you leave with the first fix whether or not you hire us.

Not ready to talk? Score your practice in 3 minutes, or get more free tools and templates.
Follow ClinicOps for one useful fix a week: LinkedIn | YouTube | X | Instagram | Facebook