HIPAA Website and Contact Form Compliance Checklist

A website privacy, tracking, contact form, vendor, and data-handling review tool for healthcare organizations

Purpose

Use this checklist to evaluate whether healthcare website forms, online scheduling tools, chat widgets, analytics tools, advertising pixels, email capture, and vendor technologies create privacy, security, consumer protection, or HIPAA-related risk. The checklist is designed for healthcare practices, ASCs, and office-based surgical suites that use public websites to communicate with prospective or current patients.

How to Use This Resource

- Complete this review before launching or revising website forms, online scheduling tools, chat tools, advertising pixels, analytics, or lead-capture workflows.
- Identify whether any website function collects, transmits, stores, or discloses patient-identifiable information or health-related information.
- Involve privacy, compliance, IT/security, marketing, web vendor, and legal counsel for higher-risk website functions.
- Document all vendor classifications, business associate determinations, consent language, tracking tools, and corrective actions.

1. Website Intake and Contact Forms

☐	Checklist item	Notes / owner
☐	Inventory every public form, including contact forms, appointment requests, consultation requests, newsletter signups, chat forms, and downloadable resource forms.	
☐	Confirm whether forms request or permit users to submit patient names, clinical details, images, insurance information, diagnoses, treatment history, or other protected health information.	
☐	Add clear warnings instructing users not to submit PHI, patient records, clinical images, insurance details, or confidential medical information through general website forms unless the form is intentionally configured for secure intake.	
☐	Confirm form submissions are transmitted, stored, and accessed through secure channels with appropriate access controls.	

2. HIPAA and Business Associate Review

☐	Checklist item	Notes / owner
☐	Determine whether the organization is a HIPAA covered entity or business associate for the relevant website activity.	
☐	Identify whether each website vendor creates, receives, maintains, or transmits PHI on behalf of the organization.	
☐	Obtain a business associate agreement before allowing vendors to handle PHI or ePHI, when required.	
☐	Review whether online scheduling, patient portals, chat tools, payment tools, CRM systems, email platforms, hosting providers, analytics tools, and form vendors require business associate analysis.	
☐	Confirm subcontractors that may access PHI are disclosed and appropriately restricted by contract.	

3. Website Tracking, Analytics, Pixels, and Advertising Tools

☐	Checklist item	Notes / owner
☐	Inventory analytics tools, cookies, pixels, tags, session replay tools, call tracking, ad retargeting, heat maps, and social media integrations.	
☐	Assess whether tracking tools collect health-related page visits, appointment requests, identifiers, IP addresses, device IDs, or other data that could become regulated or sensitive information.	
☐	Disable or restrict tracking on pages where patients may submit or view health-related information unless reviewed and approved by privacy/security leadership and legal counsel.	
☐	Confirm privacy notices, cookie disclosures, consent banners, and opt-out mechanisms accurately describe active technologies.	
☐	Review whether any tracking, advertising, or analytics tool shares information with third parties in a way that creates HIPAA, FTC, state privacy, or consumer protection risk.	

4. Security and Access Controls

☐	Checklist item	Notes / owner
☐	Confirm the website uses HTTPS, secure form transmission, strong administrative passwords, MFA where available, and limited administrative access.	
☐	Review hosting, CMS, plug-ins, forms, themes, and integrations for updates, vulnerabilities, and unnecessary access.	
☐	Confirm access to form submissions, website leads, and reports is limited to authorized users.	
☐	Document backup, retention, deletion, and data export procedures for website-submitted information.	
☐	Confirm security incidents, suspected breaches, or unauthorized access are escalated through the organization's incident response process.	

General business and compliance education only. Not legal, medical, accounting, tax, financial, regulatory, or clinical advice.

5. Privacy Notices, Consent, and Communications

☐	Checklist item	Notes / owner
☐	Confirm the website privacy policy accurately describes what information is collected, how it is used, who receives it, and how users can contact the organization.	
☐	Confirm text message, email marketing, newsletter, and lead-capture consent language matches actual use.	
☐	Verify users can opt out of marketing communications where required.	
☐	Confirm appointment or inquiry autoresponders do not include unnecessary PHI or sensitive details.	
☐	Review whether website language could imply medical, legal, financial, or regulatory advice when the page is informational only.	

6. Vendor and Contract Review

☐	Checklist item	Notes / owner
☐	Maintain a list of all website, marketing, hosting, CRM, analytics, form, scheduling, chat, payment, and IT vendors.	
☐	Review vendor contracts for data use, confidentiality, security, breach notification, subcontractors, data ownership, data return/destruction, audit rights, and termination provisions.	
☐	Confirm cyber liability or appropriate insurance coverage for vendors with data access or operational impact.	
☐	Restrict vendor use of submitted data for advertising, model training, resale, unrelated analytics, or other secondary purposes unless reviewed and approved.	
☐	Document vendor review, risk level, and approval before launching new website tools.	

7. Corrective Action Plan

Use this section to prioritize website privacy, security, vendor, or disclosure corrections.

Priority	Gap / risk identified	Owner / target date
Priority	Gap / risk identified	Owner / target date
High		
Medium		
Low		
Follow-up		

Resource Page Intro Copy

Use this checklist to review healthcare website forms, online scheduling, analytics, pixels, cookies, chat tools, privacy notices, and vendors that may affect HIPAA, data privacy, consumer protection, or website compliance risk.

Website CTA Copy

Need help reviewing website privacy workflows, forms, tracking tools, or vendor risk? Solstice Group can help organize the review process, identify operational gaps, and strengthen practical compliance controls.

Source Note

- Source note: This checklist reflects general HIPAA Privacy Rule, HIPAA Security Rule, business associate, risk analysis, and consumer health information concepts published by HHS/OCR and FTC guidance available as of 2026. It is not a substitute for legal or privacy counsel.
- Official sources consulted include HHS OCR HIPAA Privacy Rule guidance, HHS OCR Security Rule risk analysis guidance, HHS business associate guidance, and FTC Health Breach Notification Rule guidance.

Disclaimer

This resource is provided for general business and compliance education only. It is not legal, medical, accounting, tax, financial, regulatory, or clinical advice. Organizations should consult qualified legal, compliance, privacy, financial, and professional advisors regarding their specific obligations and risk profile.