Is Your Website Violating HIPAA?

Quick Reference Guide for Healthcare Marketers

Top HIPAA Website Violation Areas

1. Tracking & Analytics Issues

- Standard analytics platforms (Google Analytics, etc.) may accidentally capture PHI
- Cookies and tracking pixels often collect and store visitor data that could identify patients
- Session recording tools (heatmaps, visitor recordings) may capture form entries containing PHI
- Remarketing/retargeting tools create profiles based on medical conditions viewed

2. Form & Data Collection Risks

- Contact forms without proper encryption create PHI exposure
- Email collection that isn't properly secured violates HIPAA requirements
- Live chat systems often store conversations containing medical information
- Insurance information collection almost always contains PHI

3. Interactive Elements Concerns

- Cookie consent bars must meet PHI data protection standards
- Chat features need to meet specific security requirements
- Patient portals require HIPAA-compliant login systems
- Appointment scheduling systems contain appointment reasons and patient details
- Webinar or event registrations may collect health-related interests

4. Technical Security Requirements

- Missing HTTPS/SSL encryption on all website pages
- Insecure form submissions that don't encrypt data transmission
- Third-party plugins without proper security vetting
- Website backups storing PHI without proper protection

5. Email & Communication Vulnerabilities

- Automated emails containing website form submissions
- Insecure email storage of patient communications
- Marketing email systems without proper safeguards

6. Missing Documentation & Policies

- Inadequate privacy policy that doesn't address HIPAA specifically
- Undocumented processes for handling website-collected PHI
- No vendor inventory of third-party services accessing website data
- Missing BAA documentation (Business Associate Agreements)

Why This Matters to You

Your healthcare website isn't just a marketing tool—it's a **potential source of Protected Health Information (PHI) exposure.** If your website collects, stores, or transmits any patient information, you need to ensure HIPAA compliance to:

- *Protect patient privacy*
- *Avoid costly penalties*
- *Maintain your organization's reputation*

Benefits of HIPAA-Compliant Analytics

- **Maintain marketing insights** without risking violations
- **Protect patient data** with proper encryption and handling
- **Simplify compliance** with purpose-built tools
- **Reduce legal exposure** by preventing accidental violations
- **Continue optimization** of your digital marketing efforts safely

Quick Assessment: Do You Need HIPAA-Compliant Analytics?

Check all that apply to your website:

- ☐ Collects any patient information through forms
- ☐ Uses standard analytics tools (Google Analytics, etc.)
- ☐ Has appointment scheduling features
- ☐ Contains patient portal or login areas
- ☐ Uses marketing automation or email tools
- ☐ Employs third-party plugins or services
- ☐ Contains medical condition or treatment information
- ☐ Lacks documented HIPAA policies for website data

If you checked two or more boxes: Your website likely requires *specialized HIPAA-compliant* analytics solutions.

Interested in Next Steps? Contact Pilot Digital Today!

Don't risk costly HIPAA violations. Pilot Digital's specialized analytics service provides:

- *Compliant tracking solutions*
- *Website audit for violation risks*
- *Implementation of safe marketing tools*
- *Proper BAA agreements*

PILOT