mederi
DIGITAL

2026 HIPAA Compliance Checklist

2026 HIPAA Compliance Checklist

The "Red Flag" Question: Ask the agency, "Can we use the standard Google Maps embed on our new patient landing page?"

The Right Answer: "No, because Google won't sign a BAA for Maps, and it tracks patient IP addresses. *We should use a static image or a compliant mapping API instead."*

1. The contractual foundation (the BAA)

Before a single pixel is placed or an email is sent, the legal paperwork must be ironclad.

- □ **Signed Business Associate Agreement (BAA):** Does the agency have a standard BAA ready to sign? (If they have to "look into it," they aren't prepared).
- □ **Scope Verification:** Does the BAA cover the specific "in-scope" services they are providing (e.g., does it cover their analytics tool, their CRM, and their email server)?
- □ **Subcontractor Flow-Down:** Does the BAA explicitly state that any subcontractors they use (freelancers, third-party apps) are also bound by the same HIPAA protections?
- □ **Breach Notification Window:** Does the contract guarantee notification of a potential breach within a specific timeframe (ideally 72 hours or less)?

2. Technical Safeguards (The "Hard" Security)

In 2026, "addressable" standards are a thing of the past. These technical measures are now mandatory

- □ **Encryption at Rest & Transit:** Is all data encrypted using AES-256 (at rest) and TLS 1.3+ (in transit)?
- □ **Multi-Factor Authentication (MFA):** Is MFA enforced for every agency staff member who has access to your website backend, social accounts, or lead databases?

- □ **Audit Logging:** Can the agency produce a report showing exactly who logged in, what they viewed, and when? (Audit logs must typically be retained for 6 years.)
- □ **Automatic Logoff:** Do their systems automatically terminate sessions after a period of inactivity to prevent unauthorized access on shared devices?

3. Marketing-Specific Compliance

Marketing requires unique data handling that general IT often overlooks.

- □ **Tracking Pixel Audit:** Has the agency removed or "server-side" gated tracking pixels (Meta, Google) on pages where a user's presence implies a medical condition?
- □ **Form Security:** Are website contact forms using a HIPAA-compliant handler (e.g., JotForm Enterprise or Formstack) that encrypts the data before it's stored?
- □ **IP Anonymization:** Is IP anonymization/masking enabled in Google Analytics 4 (GA4) or other tracking tools?
- □ **De-identification for Reporting:** Does the agency strip all PHI (names, phone numbers, emails) from the performance reports they send you?

4. Operational Hygiene

Compliance is a verb, not a noun. It requires ongoing action.

- □ **Annual Risk Assessment:** Does the agency perform (and can they show you) an annual security risk assessment of their own digital environment?
- □ **Staff Training Logs:** Can the agency provide proof that its team completes HIPAA awareness training at least once a year?
- □ **Termination Protocol:** Do they have a documented process to immediately revoke access for employees who leave the agency?
- □ **Vulnerability Scanning:** Does the agency perform biannual vulnerability scans and annual penetration testing on the websites it manages?

How can Mederi Digital help get your practice compliant?

Our founders, Jerett Patterson and James Thompson, each bring nearly 25 years of experience delivering digital excellence to the medical industry's leading names. They've seen firsthand how healthcare is evolving and know that building trust is the foundation of every patient connection.

That's why they founded Mederi, headquartered in Houston, Texas, to empower healthcare professionals with tailored digital solutions that foster lasting relationships and drive real growth.

We're here to help you grow and build trust with confidence.

Schedule a call

We want to talk to you about your practice's digital experience, where it stands, where it may be vulnerable, and how a healthcare-specific partner can support long-term stability and growth.

https://www.mederidigital.com/contact-us