

HIPAA and Website Tracking: What to Check on Your Practice Website

Most practice websites run the same tools as any other business: an analytics tag, an advertising pixel, a chat widget, a scheduling plugin. On a healthcare site, some of those tools can collect information that links a person to a health condition or an appointment. That is where marketing meets privacy law.

Why this became an issue

The US Department of Health and Human Services has published guidance on the use of online tracking technologies by organizations covered by HIPAA. Parts of that guidance have been challenged in court, and the detail is still moving. State privacy laws and the Federal Trade Commission have also taken an interest in health data shared with advertisers.

The practical point does not depend on how each case ends: a practice should know what its website sends, to whom, and under what agreement.

What to check on your own site

- ☐ List every tag. Analytics, ad pixels, heatmaps, chat, video embeds, scheduling and form tools. Most sites have more than the team remembers.
- ☐ Find the sensitive pages. Appointment requests, patient portals, condition and treatment pages, and any page behind a login deserve the closest look.
- ☐ See what is sent. Page addresses, form fields and button clicks can all be passed to a vendor. A page address alone can reveal a condition.
- ☐ Check the agreements. Ask each vendor whether it will sign a business associate agreement, and what it does with the data if it will not.
- ☐ Remove what you do not use. Old pixels from past campaigns are a common finding.

Marketing can still be measured

Privacy-aware measurement is possible. Calls and form submissions can be counted without sending the content of the form. Campaign results can be tied to a channel without building audiences from health pages. It takes planning before the tools are installed, not after.