HINSHAW

From "Find a Doctor" to "Call a Regulator:" Why Hospital Websites are the Next Privacy Scandal

Includes a Three-Step Health Privacy Compliance Playbook

Privacy, Cyber & AI Decoded Alert | 7 min read

Mar 27, 2026

By: Jason J. Oliveri

On a Thursday morning, a hospital's chief marketing officer forwards you a link with a short, ominous note: "Is this us?"

The link is to a local news article. A patient claims she visited your health system's behavioral health pages, used your "find a therapist" tool, and then started seeing eerily specific ads for depression medication and online therapy on social media. The article names your system, shows screenshots of your website, and quotes an advocacy group accusing the hospital of "selling out vulnerable patients" through tracking and location data.

You anxiously scroll further and see that the reporter has spoken with a privacy researcher who points out that your site uses multiple third-party analytics scripts. One of them, the researcher notes, "can combine IP-based location, page categories like 'behavioral health,' and mobile advertising identifiers to build very sensitive profiles." The piece ends with a comment from the state attorney general's office: "We are aware of these concerns and are reviewing whether state health data and privacy laws apply."

None of this involves the electronic health record (EHR). No one "disclosed PHI" in the way you were trained to look for. Yet your CEO is now asking how your hospital became the villain in a story about tracking people who seek mental healthcare.

In 2026, some of the riskiest "health data" your hospital touches never goes anywhere near a chart. It lives instead in patient-facing websites, mobile apps, maps, pixels, software development kits (SDKs), and push notifications that quietly track where patients browse, wait, and recover.

As state "consumer health data" laws, geofencing bans, and location-focused enforcement converge with HIPAA, precise location and digital exhaust from your digital tools are being recast as health data–even when they sit

outside traditional covered entity workflows.

Health Data That Never Touches the Chart

For years, many organizations used a simple rule of thumb: if it looks like protected health information (PHI) and lives in or near the electronic health record (EHR), we worry–everything else is marketing. *That traditional approach now presents new dangers.*

States have stepped in to regulate health-related data that sits completely outside traditional HIPAA lanes. Washington's My Health, My Data Act and similar laws treat **"consumer health data"** broadly, reaching information that identifies someone's past, present, or future physical or mental health–and the inferences you can draw from location, browsing, and app use. California and other states go further by treating precise geolocation itself as "sensitive" when linked with certain services or characteristics.

These laws apply based on what you collect and how you use it, not just whether you are a covered entity. If your hospital-branded wellness app, symptom checker, or educational site tracks behavior that reveals health status or interest, you may be in scope even if you never touch a diagnosis code.

At the same time, your "digital front door" now looks a lot more like a consumer platform than a hospital information system. Patient portals, scheduling tools, and mobile apps are typically built on third-party cloud services and SDKs designed for engagement and analytics. They quietly collect IP addresses, device identifiers, clickstreams, page categories, and location data. Some of that is clearly PHI in context, some clearly is not, and a growing middle category triggers state consumer health and privacy laws even when HIPAA does not.

The practical takeaway: stop asking only "Is this PHI?" and start asking "Would a regulator or journalist look at this and say, 'That is health data'?"

Why Location Tracking Scares Patients and Regulators

Patients do not talk about "sensitive personal information." They talk about whether they feel followed.

Location tracking feels different for three simple reasons:

- **It is continuous.** Unlike a one-time form field, location tracking often runs in the background. Patients tap "Allow Location" once to get from the parking garage to the lobby and then forget they ever did, while the app keeps sending coordinates whenever it is active.
- **It bridges the physical and digital worlds.** A visit to an oncology clinic is no longer just an offline event. It becomes an input to advertising systems, personalization engines, and risk models. That feels especially sensitive around reproductive care, mental health, or other stigmatized services.
- **It implicates other people.** Location patterns reveal not only an individual's conditions, but also who they visit, where they work, and which communities they move through. "They tracked where sick people went"

lands with regulators, journalists, and juries in a way "we misconfigured a cookie banner" never will.

Regulatory Enforcement of Hospital Websites

Regulators have noticed. A recent Health Affairs study found that nearly every US acute care hospital website transmits data to third parties when patients or the public visit, frequently via third-party tracking technologies. HHS's Office for Civil Rights has issued specific guidance on online tracking, warning that information collected by pixels and similar tools on regulated entities' websites and apps can be PHI when it relates to an individual's healthcare or payment.

At the same time, laws like Washington's My Health My Data Act explicitly ban certain uses of geofencing around health facilities and treat consumer health data as a protected category in its own right.

Geofencing also consumes the headlines: drawing a digital fence around a clinic, identifying devices seen there, and using that to target ads or sell audience segments. But if you focus only on "fences," you can miss the rest of the maze. The bigger risk comes from any combination of precise location, health-related context, profiling or targeted messaging, and opaque multi-party data flows–whether or not anyone uses the word "geofence."

A Three-Step Health Privacy Compliance Playbook

The good news is that you do not need a 40-page policy or a PhD in ad-tech to get started. Start your process by following this short, three-step playbook to map out your health privacy compliance:

1. Map the Digital Front Door

Start where patients actually show up online. Inventory:

- Public-facing hospital websites and microsites.
- Scheduling tools and "find a provider" pages.
- Portals, mobile apps, telehealth, and virtual care landing pages.

For each, ask three questions:

- What trackers and SDKs are present?
- Where do they send data?
- Do any of those flows touch behavioral health, reproductive care, or other obviously sensitive services?

You may not love the answers, but you will finally see the problem you are being asked to own.

2. Set Simple Rules for "Sensitive Signals"

Instead of arguing about definitions, define a short list of sensitive signals you treat as high risk by default: precise geolocation in health-related contexts, wearable and biometric data, mental health app usage, reproductive health tracking, and AI-generated health risk scores.

Then apply simple, memorable rules:

- We do not build or buy audiences based on visits to our facilities or other sensitive health locations.
- We do not share precise location information from our properties with third parties for their own advertising or profiling.
- Any new use of sensitive signals (especially location) for personalization or AI modeling gets a privacy review before it ships.

Build one extra question into existing intake forms: "Does this involve precise location or other sensitive signals around patient journeys?" Then, route "yes" answers to a small cross-functional group. No new committee, just a better reflex.

3. Tame the Vendor Stack (Starting with the Worst Offenders)

A lot of your risk sits in contracts you did not draft.

SDK and platform agreements often reserve broad rights to use "de-identified" or "aggregated" data–including location and interaction data from your patients–for the vendor's own analytics, product development, or advertising. Your Notice of Privacy Practices may promise one thing while a vendor's terms quietly say another.

You do not have to renegotiate everything at once. Start by creating a short location and health signals rider that:

- Prohibits the sale or secondary use of precise location data from your properties for unrelated advertising or profiling.
- Bans geofencing and sensitive location profiling without explicit instructions from you.
- Requires compliance with applicable state consumer health and privacy laws.

Prioritizing that rider for:

- Renewals and new deals involving digital health, marketing, analytics, and location services.
- Vendors that show up in your tracking inventory on sensitive pages.
- Vendors implicated in any complaint or incident about "weird ads after visiting our site."

It is not glamorous, but it is where quiet risk becomes loud headlines.

Where Hinshaw Plugs In

Hinshaw's work with health systems lives at this intersection of HIPAA, state consumer health laws, and the messy reality of pixels, SDKs, and location data. **In practice, that usually means helping clients:**

- Turn "Is this us?" moments into concrete inventories and risk maps.
- Design a sensitive signals framework that leadership can remember and teams can actually use.
- Clean up the worst offenders in the vendor stack, so your public promises and your contracts finally match.

Regulators are already treating location tracking around health journeys as regulated health data. The question is whether your next headline is a case study in what went wrong or a more favorable news story about the great work your organization is doing because you saw this coming and tightened the compliance screws first.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Healthcare

Healthcare Regulation, Compliance & Licensing

Hospitals, Rural Health Systems & Service Providers

Regulatory & Compliance

Website Data Privacy

Related Insights

Compliance Considerations for GDPR Consent in Biotech Clinical Research