
— HEALTH PRIVACY LITIGATION

Who Else Was Watching

Tracking Pixels, Patient Portals, and Health Privacy Litigation

BY MICHELLE CARROLL · FOUNDER & CEO, LEXCURA SUMMIT

If you've booked an appointment or logged into a patient portal, the site may have been running tracking pixels, snippets of code from companies like Meta and Google that measure advertising and site use. On a retail site that's routine. On a healthcare site, the same code can reveal that an identifiable person, tied to an IP address, device, or social media account, looked up an oncologist, scheduled at an abortion clinic, searched for HIV treatment, or logged into a portal and opened test results.

After journalists reported in 2022 how common these pixels were on hospital websites, lawsuits followed, and they've kept coming, spreading from big systems to smaller providers and specialty clinics. Advocate Aurora Health settled a class action for about \$12.2 million, Novant Health for \$6.6 million, and Mass General Brigham resolved a related tracking case for \$18.4 million. Courts have been certifying classes more readily, which pushes defendants toward earlier settlement.

THE FEDERAL GUIDANCE, AND ITS LIMITS

HHS's Office for Civil Rights issued a bulletin in December 2022, updated in March 2024, saying that when a HIPAA-covered provider's tracking technology sends individually identifiable health information to a vendor, that's a disclosure of PHI requiring either a business associate agreement or patient authorization. Many tech vendors won't sign BAAs.

The American Hospital Association and others sued. On June 20, 2024, a federal court in Texas (*American Hospital Association v. Becerra*) held that OCR had overstepped by treating the combination of an IP address and a visit to a public, unauthenticated page about a health

condition as PHI on that basis alone. That narrowed the guidance for public pages. It didn't address authenticated pages like patient portals, where the visitor is logged in and clearly a patient. Tracking there remains a serious problem.

HIPAA doesn't give patients a private right to sue, so plaintiffs rely on other law: federal and state wiretap statutes (especially in all-party-consent states, with California's Invasion of Privacy Act used heavily), state consumer protection laws, newer health privacy statutes like Washington's My Health My Data Act (effective March 31, 2024, with a private right of action), and common-law privacy and breach-of-confidence claims built on the patient-provider relationship.

The FTC has been active against digital health companies outside HIPAA: GoodRx in 2023, the first enforcement of the Health Breach Notification Rule, and BetterHelp the same year for sharing health data for advertising.

WHY CLINICAL KNOWLEDGE MATTERS IN A PRIVACY CASE

The harm depends on what the data reveals. A pixel on an "about us" page reveals almost nothing. A pixel that fires when someone clicks "schedule" on a gender clinic, addiction treatment, oncology, or fertility page reveals a great deal. Some categories, like substance use disorder treatment records, have heightened federal protection of their own. Mapping each page and portal function to the clinical service behind it helps define the class, show which patients were most exposed, and explain the harm.

Individual stories matter too. Some plaintiffs say they began seeing ads tied to a condition they'd only researched on their provider's site. Documenting what they looked up, when, and what followed supports individual claims.

A FICTIONAL CASE

A regional health system has a Meta pixel on its public pages and, through a configuration error, inside its patient portal. For two years, when patients log in, message their doctors, or view results, the pixel sends data about those actions to the vendor, including which portal section they visited. A researcher finds it, the system removes it and sends breach notices, and a class action follows.

Which laws apply and whether there was consent are legal questions. What the pixel sent, when, and to whom are technical questions. What those portal sections reveal about patients' health, and which categories of care are most sensitive, are clinical questions, and they give the data its meaning.

WHAT WERE PATIENTS TOLD?

Consent is at the heart of many claims. What did the privacy policy say? What did clicking “accept” on a cookie banner actually agree to? Did the portal terms mention third-party tracking? Plaintiffs often compare the HIPAA notice of privacy practices with what the pixel actually did. Get the versions in effect at the time. A policy rewritten after discovery says nothing about what patients saw before.

PROVING HARM

Standing and damages are hard in privacy cases. Since *TransUnion LLC v. Ramirez* (2021), courts have split on whether people whose data was shared, but who can’t show a concrete loss, can sue in federal court. Some state statutes set per-violation damages, which changes the math entirely. Here again, sensitivity matters: disclosure that someone sought addiction, HIV, or mental health care is far easier to see as real injury than disclosure that someone checked visiting hours.

BEYOND THE PIXEL

Session replay tools, third-party chatbots and scheduling assistants, and AI tools that transcribe or summarize patient conversations raise the same questions: what leaves the provider, where it goes, what the vendor can do with it, and whether patients agreed.

FOR PROVIDERS

Many systems have stripped third-party tracking from their sites and portals or moved to tools that don’t share identifiable data. Audit what’s running, especially on service-specific pages and anywhere patients log in. Include the marketing and IT people who actually manage the site, since tags often get added without compliance knowing. Make sure vendor contracts limit what vendors can do with data, and that your privacy notice matches reality. And remember that discovering a pixel may trigger HIPAA and state breach notification deadlines.

RECORDS WORTH REQUESTING

- Website and portal code and tag manager configurations over time
- Vendor contracts, data sharing agreements, and any BAAs
- Privacy policies, notices of privacy practices, cookie banners, and portal terms, with version dates
- Internal assessments, breach investigation reports, and notification letters
- A map of affected pages and portal functions and the clinical services behind them
- For individual plaintiffs: what they searched, scheduled, or viewed, and what followed

SOURCES

- HHS OCR, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 2022; updated Mar. 18, 2024)
- *American Hospital Association v. Becerra*, No. 4:23-cv-01110 (N.D. Tex. June 20, 2024)
- Wash. Rev. Code ch. 19.373 (My Health My Data Act)
- FTC actions against GoodRx (2023) and BetterHelp (2023)
- *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021)
- Curve Compliance, “Healthcare Pixel Lawsuit Settlements: Mid-2026 Roundup”; HIPAA Journal pixel settlement coverage

This newsletter is for education only and isn't legal advice. The case is fictional.

ABOUT LEXCURA CLINICAL INTELLIGENCE

Lexcura Clinical Intelligence provides integrated clinical and regulatory analysis for attorneys handling healthcare litigation. If you have a health privacy case and need the affected pages and portal functions mapped to the care they reveal, we'd welcome the conversation.

Michelle Carroll

FOUNDER & CEO, LEXCURA SUMMIT

