CLIENT ALERTS & INSIGHTS

Emerging Enforcement Trends in Digital Health Data Privacy: Lessons from Washington's My Health My Data Act, FTC vs. Hims & Hers and UCHealth Enforcement Actions

AUGUST 31, 2026

Authors: Ryan T. Sulkin, Lauri A. Cooper, Kathrin "Kat" Zaki

Featured Practices: Data Privacy & Cybersecurity, Healthcare

Key Takeaways

- Regulators and private plaintiffs are increasingly scrutinizing how healthcare, digital health and consumer-facing companies collect, share and protect health-related data, particularly through website tracking technologies and third-party vendor relationships.
- Recent actions against Hims & Hers, Amazon and UCHealth demonstrate that organizations can face significant enforcement and litigation risk even when using data sharing practices common in the marketplace. Regulators are also taking an increasingly broad view of what constitutes "health information," expanding potential exposure beyond traditional HIPAA-covered data.
- Organizations should proactively review their tracking technologies, data-sharing practices, privacy disclosures and vendor agreements to ensure they align with evolving regulatory expectations. A comprehensive data governance and privacy compliance strategy can help reduce the risk of enforcement actions, class action litigation and reputational harm.

Overview and Recent Enforcement Activity

The digital health sector faces a rapidly intensifying regulatory and litigation environment with respect to data privacy, unauthorized data sharing and deceptive consumer practices. Two recent matters including the FTC's joint action against Hims & Hers Health, Inc. and a class action against University of Colorado Health (UCHealth), illustrate the breadth and seriousness of this trend.

On July 29, 2026, the Federal Trade Commission (FTC), along with the State of California and the State of Utah, filed a complaint against Hims & Hers Health, Inc. (Hims), a major telehealth company, in federal court in San Francisco. The government says Hims:

-

Promised users their health information would stay “private” and be seen “only by medical providers” but then secretly shared that data with advertising companies like Meta (Facebook) and Snap (Snapchat).

- Used tracking pixels and other tools to send information about users’ health conditions (including mental health, sexual health and prescriptions) to ad platforms.
- Charged consumers for prescriptions and subscriptions without their clear consent.
- Made it extremely difficult for consumers to cancel subscriptions.
- The government is seeking financial penalties and an injunction, among other remedies.

On August 5, 2026, a patient filed a class action lawsuit in the U.S. District Court for the District of Colorado against University of Colorado Health (UCHealth). The complaint alleges the following:

- UCHealth installed Meta’s tracking pixel on its website, including a tool patients use to find doctors.
- The pixel secretly sent patients’ health-related searches (symptoms, conditions, doctor specialties, appointment information) to Meta/Facebook-along with information that could identify the patient (like IP addresses and Facebook IDs).
- Patients never consented to this, and UCHealth never told them it was happening.
- The lawsuit also alleges UCHealth may have used the same tracking technology on its patient portal (where patients message their doctors, view test results, etc.).

The plaintiff argues this violates the Electronic Communications Privacy Act (a federal law that makes it illegal to intercept private electronic communications) and HIPAA (the law protecting patient health data). UCHealth serves nearly 3 million patients per year, so the potential class could be very large.

On February 10, 2026, a consumer filed a class action suit against Amazon.com, Inc. and Amazon Advertising, LLC (collectively “Amazon”) in the U.S. District Court for the Western District of Washington alleging violations of Washington State’s My Health My Data Act (“MHMDA”). The complaint alleges that:

- Amazon unlawfully harvested sensitive location data from users through advertising software integrated into third-party mobile apps. Amazon’s advertising software, known as a “software development kit,” or SDK, is licensed to and “runs in the background of thousands of mobile apps” and “covertly withdraws sensitive location data” that cannot be completely anonymized.
- Amazon violated Washinton’s MHMDA by failing to obtain proper consent or provide adequate disclosure regarding the collection and sharing of consumer health data.

Together, these actions reflect an enforcement landscape in which both government regulators and private plaintiffs are holding healthcare entities accountable for the use of web-based tracking technologies that expose sensitive health data to unauthorized third parties.

Why This Matters: The Bigger Picture

These enforcement actions and class action lawsuits are not isolated cases. Several patterns across these lawsuits signal broader enforcement trends.

- **Tracking pixels are now a top legal risk.**

Both the UCHealth and Hims cases involve Meta's tracking pixel, a tiny piece of code that websites install to track visitors' activity and send data back to Facebook for advertising purposes. SDKs or similar technologies also track and share data that could fall under the definitions of "health data" under various state and federal privacy laws. These tools, once viewed as routine marketing infrastructure, are now a source of regulatory and litigation risk for healthcare and online retail entities if the pixels result in third party sharing of sensitive consumer health information.

- **"Health data" is being defined very broadly.**

You don't need to be a HIPAA-covered entity to get in trouble. If someone visits your website seeking health-related information (like browsing treatments for weight loss or searching for a psychiatrist), the data generated by that visit may count as "sensitive health information" especially if it can be linked back to an identifiable person and covered under state privacy laws or the FTC's confidentiality requirements.

Other states are following Washington's MHMDA, including Nevada who adopted a mirror image law, while Connecticut added certain pieces from MHMDA to its Data Privacy Act. New York has its own version of MHMDA making its way through the New York law making process.

- **Private lawsuits add another layer of risk.**

While the Hims action is a government enforcement matter filed jointly by the FTC, California and Utah, the UCHealth case is a proposed class action by a private plaintiff. The Washington MHMDA is also a private plaintiff. The proliferation of pixel-tracking litigation demonstrates that companies face risk not just from federal and state government entities but also from individual patients and consumers.

- **Overpromising privacy protections and underdelivering can backfire.**

Hims and UCHealth made privacy promises to users. When their actual data practices contradicted those promises, it became a central basis for legal liability. Companies that overclaim privacy are at greater risk than those that are transparent about data sharing.

- **The whole consumer experience is under scrutiny.**

The Hims case isn't just about data, it also challenges deceptive billing, unclear subscription terms and difficult cancellation processes. Regulators are looking at the entire digital health customer journey, making it more important than ever to reevaluate the lifecycle of data in your company.

Takeaways & Recommendations: What Should You Do Now?

Digital health companies, healthcare providers, retailers and organizations handling health-related data should consider the following steps to mitigate enforcement and litigation risk:

1. **Audit your tracking technologies now.**

Check every pixel, tag, cookie, SDK and API on your website and apps. Identify exactly what data they collect and where it goes. If any of these tools send health-related or personally identifiable information to advertising platforms, consider removing or restricting them immediately.

2. **Be honest in your privacy communications.**

Don't overpromise "privacy" or "discretion" if you're widely sharing data with third parties. Make sure your privacy policies, website language and marketing materials accurately reflect what you actually do with user data.

3. **Tighten your vendor relationships.**

If you work with advertising or analytics companies, make sure your contracts clearly limit what they can do with your users' data. If HIPAA applies to you, ensure you have proper Business Associate Agreements in place with vendors that specifically address narrow parameters for third party data sharing.

4. **Think broadly about what counts as "health data."**

Don't limit your definition to traditional medical records. If a user's activity on your site could reveal anything about their health (e.g., conditions they're researching, treatments they're browsing, doctors they're looking for), treat that data as sensitive.

5. **Fix your consent and disclosure practices.**

Give users clear, upfront information about data collection and sharing and get true informed consent (not buried-in-fine-print consent). If you use subscription models, make sure the terms are obvious and the process for cancellation is clear.

6. **Plan for multistate compliance.**

Different states have different rules. HIPAA, the FTC Act, state privacy laws (like the California Consumer Privacy Act) and consumer protection statutes may all apply to you simultaneously. Build a compliance program that addresses all of them.

7. **Get leadership involved.**

Make data privacy a board-level issue. Ensure your leadership understands the risk and is engaged in oversight of your compliance program.

8. **Stay alert.**

The regulatory environment is changing fast. Monitor FTC enforcement actions, new state laws, and litigation trends so you can adapt before problems arise.

Key Insights

- Digital health and healthcare technology companies are increasingly being targeted over how they handle patient and consumer data.
- The FTC joint action against Hims & Hers, plus two recent class action suits against Amazon in Washington and UC Health system in Colorado, illustrate a broader pattern of enforcement and litigation targeting several data privacy practices facing increased legal scrutiny.
- Tracking pixels (small bits of code that send user data to advertising companies like Meta/Facebook), and third-party data sharing are emerging as a major source of legal risk.
- Regulators are taking an expansive view of what constitutes “health information,” and even if your organization isn’t covered by HIPAA, regulators may still consider your users’ health-related data “sensitive” and hold you accountable for sharing it under state and FTC rules.
- Joint federal-state enforcement actions signal coordinated regulatory scrutiny, including state attorneys general partnering with the FTC.
- Companies that promise “privacy” or “discretion” but share data with ad platforms face serious enforcement risk and must reassess their use of website tracking technologies, vendor relationships and privacy representations to patients and consumers.
- Now is the time to audit your data practices because robust data governance, privacy compliance programs and proactive vendor management are essential to mitigate enforcement and litigation risk.

Benesch’s Healthcare and Data Privacy teams are available to assist clients in navigating these complex issues. Please contact Ryan Sulkin (rsulkin@beneschlaw.com) at 312.925.3405, Lauri Cooper (lcooper@beneschlaw.com) at 419.266.4521, or Kat Zaki (kzaki@beneschlaw.com) at 646.777.0040 for any follow up questions.