DATA PRIVACY & GOVERNANCE HUB

Novartis Lawsuit Reveals Gray Area in Patient Data Privacy

APRIL 24, 2026

Key Takeaways

- A lawsuit filed against Novartis alleges that the company used invisible tracking tools on its websites to collect and pass patients' sensitive health information to third parties without their knowledge or consent.
- This case highlights a regulatory gap in the application of existing privacy law to digital data collection on pharmaceutical websites and exposes a potential HIPAA violation.
- Stronger transparency measures, like user consent requirements and mandatory disclosure of third-party data recipients, have been proposed to address these gaps.

What Happened

Novartis, the leading global medicines company based in Switzerland, is being sued by a patient in a New Jersey district court over its website data-sharing practices. The patient alleges that Novartis installed tracking tools to collect sensitive health information, including data on medical conditions, prescriptions, and medical expenses, and then shared that data with unauthorized third parties without the patient's consent.

The patient maintains that she only discovered that the company had installed invisible tracking tools after she began seeing targeted ads related to her medical condition on other sites. Novartis is among the most prominent big pharma groups targeted by this type of litigation, with patients now left questioning whether they are prioritizing profits over patient privacy.

Privacy and Governance Concerns

The company's websites capture sensitive health information and personally identifiable information submitted by patients through invisible tracking pixels and other tools, which are then transmitted to third parties such as Google and Meta. These electronic mechanisms pose significant risks, including the unauthorized disclosure of medical conditions to third-party corporations, potential emotional harm to affected individuals, infringement of medical privacy rights, and the exploitation of sensitive health data for targeted advertising without the user's informed consent.

This also enables health profiling across multiple platforms, allowing advertisers to target users based on search history and profit from it. With each additional third party, the risk of a breach, misuse, or further unauthorized sharing increases. The regulatory landscape is unsettled, and it is unclear whether pixel-tracking data from public webpages constitutes protected health information under HIPAA (Health Insurance Portability and Accountability Act), potentially revealing a significant loophole in current policy.

Why It Matters / Policy Considerations

Current safeguards may not adequately address the growing use of digital tracking tools on healthcare websites, and this case demonstrates how HIPAA's protections fail to meaningfully extend into the digital space. This leaves patients vulnerable to exploitation, and regulators should consider expanding the definition of protected health information to web spaces. Additionally, consent should be required before deploying tracking tools, particularly on healthcare websites. Transparency would be strengthened through this, as well as mandatory disclosure of all third parties purchasing data.