Insights: Publications

Uncertain Boundaries: How Courts and Regulators View the Sharing of Health-Related Article Titles

August 28, 2025

Written by **Tatum Andres** and **Meghan K. Farmer**

Recent regulatory actions and court decisions highlight growing uncertainty over whether sharing article title data from webpages amounts to disclosure of sensitive health information under privacy laws.

Consider a consumer casually browsing the open internet, not logged into a hospital portal, and clicking on articles such as “Managing Life After a Diabetes Diagnosis” or “Understanding Early Symptoms of Depression.” If the URL or article title is then transmitted to an advertising platform through a cookie or pixel, does that constitute disclosure of sensitive health information?

California's Attorney General has suggested that it can, reasoning that reading content linked to medical conditions may itself reveal sensitive personal details. Federal courts, on the other hand, have been more cautious, finding that sharing health-related data collected on a public site does not qualify as disclosure of protected health information if the online tracking technologies on the webpages do not have access to information that relates to any individual's past, present, or future health, health care, or payment for health care.

This divergence leaves businesses and publishers uncertain about whether sharing article titles or page-level browsing data connected to health topics could violate state or federal privacy requirements.

California AG Enforcement: Healthline Complaint

In a recent enforcement action, the California Attorney General alleged that Healthline's use of cookies and tracking technologies violated both the California Consumer Privacy Act (CCPA) and the Unfair Competition Law (UCL).[i] The complaint focused on how article titles and page-level browsing data were shared with advertising providers.

The AG characterized these disclosures as sensitive personal information under the CCPA, particularly where the content suggested that the user had already been diagnosed with a serious condition. Examples included article titles such as *“The Ultimate Guide to MS for the Newly Diagnosed”* and *“Newly Diagnosed with HIV? Important Things to Know.”*

Two aspects of the AG's position stand out:

- **Broader conception of health information:** The complaint suggests that merely reading articles that are strongly associated with serious health conditions may itself be considered disclosure of sensitive health information, even in the absence of direct identifiers or clinical records.
- **Disclosure expectations:** While Healthline's privacy policy included general language stating that it "may provide consumers' information to advertising providers for purposes of targeted advertising," the AG faulted the company for failing to disclose that specific article titles would be transmitted.

The Healthline complaint therefore signals that California regulators may expect companies to take an expansive view of sensitive personal information, one that goes beyond the more traditional definitions used under federal law.

Federal Court Perspective

By contrast, several courts have dismissed claims alleging that the use of tracking technologies on websites resulted in the disclosure of protected health information in violation of federal law. The webpages at issue in those cases contained content such as information about melanoma treatment options, details about specific doctors, search results for the phrase "intestine transplant," a wife's blog post about her husband's cancer diagnosis, and other publicly available health information.

Courts have reasoned that merely browsing or searching health-related websites is insufficient to constitute the disclosure of "individually identifiable health information" under HIPAA or to trigger liability under state or federal wiretap laws. These rulings emphasized that:

- Interactions with publicly accessible webpages do not amount to disclosures of personal medical histories.
- The link between a person's browsing activity and their actual health status is too tenuous to support a claim that HIPAA-protected information was transmitted.
- A meaningful distinction exists between activity on consumer-facing health websites and direct communications between patients and providers within clinical or hospital portals.

These decisions reflect the more limited approach federal courts have taken in evaluating whether online activity constitutes a disclosure of protected health information.

HIPAA Guidance on Tracking Technologies

Guidance from the Department of Health and Human Services (HHS) on the use of tracking technologies further underscores the complexity. HHS has explained that tracking on unauthenticated webpages is generally not regulated under HIPAA, unless the tracking technologies have access to information that is both identifiable and related to an individual's past, present, or future health or health care.[ii]

Examples provided by HHS clarify that:

- A user visiting a hospital webpage about job postings or visiting hours does not implicate HIPAA, even if the visit can be linked to an IP address or device.
- A student researching oncology services for a paper is not disclosing protected health information.

Implications for Companies

The regulatory and judicial divergence over the treatment of health-related article titles reflects a broader and unresolved tension in privacy law, which companies must wade through carefully, in real time, while guardrails are still being put into place around emerging technologies. Businesses today cannot wait for legal clarity before making operational decisions. Instead, they must navigate a patchwork of enforcement actions, court rulings, and regulatory guidance that often point in different directions.

On one hand, California regulators have adopted an expansive view that suggests merely reading articles about medical conditions could amount to disclosure of sensitive health information if those article titles or URLs are shared with advertising platforms. On the other hand, federal courts have been more restrained, emphasizing that publicly accessible browsing activity is too far removed from actual clinical data or personal health histories to qualify as protected health information under HIPAA.

This uncertainty is not limited to health care companies. Any business or publisher that posts content about medical conditions, wellness, or even general lifestyle advice should take notice. A recipe blog with articles about managing low-sodium diets, a news outlet reporting on cancer treatments, or a university page describing mental health resources could all be swept into this debate if tracking technologies on their sites transmit article-level data to third parties. What is at issue is not whether the company is a hospital or health-related entity, but whether the browsing behavior itself reveals information regulators might consider sensitive.

The implications also extend beyond the health space. If the California Attorney General is willing to take the position that sharing health-related article titles constitutes the disclosure of sensitive personal information, it is not difficult to imagine similar arguments being made for other categories of data. Consider a consumer reading articles titled *"How to File for Bankruptcy"* or *"Tax Benefits for Families Facing Foreclosure."* If those titles are shared with advertisers, do they reveal sensitive financial information in a way that privacy law should protect? The logic is parallel. Just as reading about a chronic condition could suggest a diagnosis, reading about bankruptcy or foreclosure could suggest financial distress.

Conclusion

For companies, the lesson is clear: the boundaries of what regulators and courts will consider sensitive information are shifting and inconsistent. Regulators may continue to push expansive interpretations, while courts may continue to narrow them, but businesses must prepare for both. Updating privacy disclosures to address article-level tracking, minimizing the sharing of sensitive browsing data, and monitoring enforcement trends will be essential steps in reducing risk. The law may eventually catch up to technology, but in the meantime, companies must act as if the broader standard could apply.

---

[i] *The People of the State of California v. Healthline Media LLC,* case number CGC-25-626794, in the Superior Court of the State of California, County of San Francisco (Complaint: 7/1/25).

[ii] Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Related People

Tatum Andres

t 312.628.7183

tandres@ktslaw.com

Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com