Health Tech Regulatory Trends To Watch In 2025

By **Thora Johnson, Georgia Ravitz and Amy Joseph** (January 1, 2025)

Thora Johnson

Georgia Ravitz

Amy Joseph

With a change in administration and the release of some long-awaited rules, the healthcare industry is bracing for both regulatory developments and more litigation that will have a significant impact this year.

In particular, the continued market interest in technology-enabled delivery of healthcare, fueled in part by a focus on responsible use of artificial intelligence, is certain to grab the attention of federal and state lawmakers alike, and the ongoing use of advertising technology will continue to give raise to lawsuits. This article identifies key trends to watch.

Health Data Developments

Despite the change in administration, we expect to see the flurry of activity around health data from last year continue into 2025. Here are a few of the developments to track in the new year.

Wiretap and Pixel Tracking Claims

This year, we saw hundreds of class actions filed targeting entities for their use of ad tech. While these lawsuits implicate industry agnostic privacy statutes, we have seen them used especially effectively in the health context.

For example, the claim that URL-tracking in the context of searches related to mental health constitutes content of a communication under the California Invasion of Privacy Act recently survived a motion to dismiss.[1]

Additionally, in Castillo v. Costco in November, the U.S. District Court for the Western District of Washington accepted economic devaluation of health data through pixel tracking as an injury at the motion to dismiss stage.[2] We will be following how these cases effect litigation risk over the coming year.

Increasing State Legislation on Health Data and a Focus on Reproductive Health

One statute that we are closely monitoring is the Consumer Health Information Privacy Protection Act,[3] introduced in Washington, D.C., in late July. If enacted, the act would, among other things, require companies to seek affirmative consent before sharing covered data and would be subject to a private right of action.

New York will be considering a similar statute that would require companies to solicit written consent for health data use beyond necessary processing.[4] These statutes are modeled after state laws enacted in the wake of the U.S. Supreme Court's 2022 decision in Dobbs v. Jackson Women's Health Organization, such as Washington's My Health My Data[5] and Nevada's S.B. 370.[6]

We expect to see the Democratic-led states continue to pass legislation to protect the confidentiality of reproductive health and gender-affirming care. For example, last year, California added heightened security requirements to medical information related to gender-affirming care and reproductive health.[7] Michigan is currently considering S.B. 1082,[8] the first health data privacy act scoped to reproductive data, and more states may follow suit.

Additional Protections Implemented for Biometric and Neural Data

We expect states to continue to extend additional privacy protections to biometric and neural data. Colorado has amended its comprehensive privacy act to include specific provisions for the retention and control of biometric data similar to those in Illinois, but without a private right of action.[9]

The bill goes into effect July 1, and we will be looking toward the Colorado attorney general's office for rules implementing the act in the lead-up. California's law adding neural data as a category of sensitive data will also go into effect this year, and other states may follow suit with similar amendments.[10]

General State Privacy Legislation That May Sweep in Health Data

We'll be watching for a shift toward a substance-based approach to data minimization.

In Maryland, the Online Data Privacy Act is set to take full effect in October.[11] The statute would only allow an entity to collect sensitive data, like health data, when it is strictly necessary to service a consumer's requests. While it is possible that soliciting consent will satisfy this requirement, this point of implementation remains ambiguous.

Movement away from process-based language has spread beyond the Maryland statute. We have seen bills with similar language proposed in both Vermont[12] and Maine.[13] This year, we will be paying close attention to how the Maryland bill is enforced as a cue for how similar statutes may play out if enacted during this next legislative cycle.

More Security Standards Around Health Data to be Issued

When it comes to the federal regulatory space, we will be closely monitoring the U.S. Department of Health and Human Services' proposed rulemaking around cybersecurity of protected health information for entities regulated by the Health Insurance Portability and Accountability Act.[14]

The rule itself has yet to be released, but some expect it to codify voluntary standards that HHS proposed in a 2023 concept paper.[15] We will be following the progression of this rule through the HHS administration shift.

FTC's Appetite for Continued Enforcement Actions Against Ad Tech Remains Unknown

While privacy is a bipartisan issue, it seems unlikely that we'll see the Federal Trade Commission adopt a final rule on commercial surveillance.[16] More likely, though, is we'll see the FTC continue to protect consumers from deceptive use of ad tech that jeopardizes the privacy and security of their most sensitive information, including health data.

Regulations Affecting the Telehealth Industry

Historically, under the Controlled Substances Act, healthcare providers were required to conduct an in-person examination before they could prescribe controlled substance medication virtually, narrow exceptions applied.

In March 2020, in response to the pandemic, the U.S. Drug Enforcement Administration temporarily waived this requirement, and a number of digital health companies started offering virtual treatment that included controlled substance prescribing.

Stakeholders have been waiting anxiously for the DEA to issue permanent standards going forward, including delivering on a long overdue exception in the context of the practice of telemedicine.[17]

The DEA issued proposed standards in 2023[18] that were met with extreme backlash, due to concerns about restricting access to care, and a second attempt to issue proposed standards in 2024 also failed.

The DEA has stated that 2025 will be the year that it establishes final rules.[19] These rules could have an existential impact on many digital health companies operating today.

FDA Approval of Digital Therapeutics

The U.S. Food and Drug Administration has been approving digital therapeutics in increasing numbers, and we expect this trend to continue and grow exponentially.

Digital therapeutics are software-based medical devices that use evidence-based interventions to treat, manage or prevent diseases and disorders. Such software applications can be designed to be used in combination with a conventional pharmaceutical or biological to provide a therapeutic effect for the individual.

Digital therapeutics can address disease management through supporting lifestyle changes and also utilize algorithms to tailor dosing. Current investigations of digital therapeutics include measuring the patient's biological levels for disease management and pairing digital therapeutics with biosensors to allow for the monitoring of biological levels as a marker for treatment efficacy.

Digital therapeutics are a nascent and expanding area to address health issues holistically. With the incoming administration, we anticipate a more concerted focus on and encouragement of holistic, functional and behavioral medicine and expect applications and approvals for digital therapeutics to surge.

State-Level Oversight of AI

Finally, significant legal developments are expected with respect to the development and deployment of AI in healthcare.

We expect to see further oversight emerge around transparency in the use of AI, following on legislation out of both Utah and California in 2024 that impose heightened requirements on certain healthcare professionals in the use of generative AI, along with broader, comprehensive legislation out of Colorado that affects healthcare as well as other industries.[20]

It is possible that, much like other highly regulated areas, a patchwork of varying state-

level requirements will emerge in the near future that can create additional complexities for companies operating on a national level.

Thora Johnson, Georgia Ravitz and Amy Joseph are partners at Orrick Herrington & Sutcliffe LLP.

Orrick partner Jeremy Sherer and law clerk Tom Zick contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] M.G. v. Therapymatch, Inc., No. 23-CV-04422-AMO, 2024 WL 4219992, *4 (N.D. Cal. Sept. 16, 2024)

[2] Castillo v. Costco Wholesale Corp., No. 2:23-CV-01548-JHC, 2024 WL 4785136, *8 (W.D. Wash. Nov. 14, 2024)

[3] Washington DC Consumer Health Information Privacy Protection Act, C.B. 25-930, 25th Council Period (2024).

[4] New York Health Information Privacy Act, S.B S158, 2023-2024 Legislative Session (2024).

[5] Rev. Code Wash. § 19.373.

[6] Nev. Rev. Stat. § 603A.525.

[7] A.B. 352, 2022 - 2023 Legislative Session (2023).

[8] S.B. 1082, 102nd Legislature (2024).

[9] H.B. 24-1130, 74th General Assembly (2024)

[10] Cal. Civ. Code § 1798.140.

[11] Maryland Online Data Privacy Act of 2024, HB 567, 446th Session of the General Assembly (2024).

[12] H.B. 121, 2023- 2024 Legislative Session (2024)

[13] Maine Data Privacy and Protection Act, HP 1270, 131st Legislative Session (2024).

[14] Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 45 C.F.R. § 160 (2024)

[15] U.S. Dep. Of Health and Human Services, Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services (2023).

[16] Commercial Surveillance and Data Security 16 C.F.R. § 1 (2022).

[17] Ben Leonard, DEA Eyeing Substantial Limits to Telemedicine Prescribing, Politico, Aug 28, 2024.

[18] See DEA, "DEA and HHS Extend Telemedicine Flexibilities Through 2024" (Oct. 6, 2023).

[19] See DEA, "DEA and HHS Extend Telemedicine Flexibilities Through 2025" (Nov. 15, 2024).

[20] Utah AI Act, S.B. 149, 2024 4th Special Legislative Session (2024).