The Evolving Landscape of U.S. Health Data Privacy



Where We Are in 2026

A Subsidiary of

Introduction

Over the past year, health data privacy officially moved from an emerging regulatory trend into a central operational consideration for healthcare advertising agencies, media buyers, ad tech companies, and brand strategists. What began with pioneering standalone statutes like Washington's My Health My Data Act (MHMDA) and Nevada's SB 370 has broadened in 2026 into a complex landscape of state-level requirements. As states operationalize dedicated health privacy laws or strengthen sensitive data protections within omnibus privacy frameworks – such as in California, Maryland, Minnesota, Connecticut, and Virginia – the line between healthcare marketing and standard digital advertising is becoming increasingly blurred.

2026 Continues Trending from Entity to Content

Historically, health privacy was confined to the federal HIPAA framework, which focuses on "covered entities" like hospitals, clinics, and health plans. Modern state-level health data privacy laws enacted since 2023 have fundamentally redefined this approach, shifting the regulatory trigger from HIPAA-covered entities to any data containing health-related information. This past year with no new specific health data privacy laws passed or new novel approaches taken up, state continues to nibble around the edges of changes seen over the past few years.

Under these statutes, "consumer health data" encompasses any personal information linked or reasonably linkable to a consumer's physical or mental health status. This explicitly includes derived data—such as diagnostic inferences, reproductive health indicators, precise location data near care facilities, and targetable health interests. This shift places legal liability directly on agencies and advertisers utilizing behavioral audience data, which now encompasses:

- **Biometric & App Data**: Information sourced from fitness trackers, wellness apps, and personal health monitoring tools.
- **Inferred Health Interests**: Custom audience segments built from browsing history, symptom web searches, or online content interactions.
- **Precise Geofencing:** Ad targeting triggered by virtual perimeters drawn around medical clinics, pharmacies, or care facilities.

Core Operational Impacts on Healthcare Marketing

The evolving state privacy framework has significantly altered how digital campaigns are executed, ad-tech stacks are evaluated, and risk is managed. Recent key operational shifts include:

- **Heightened Risk Surrounding Tracking Pixels:** Standard tracking pixels (such as Meta, Google, and third-party ad-tech tags) deployed across healthcare, wellness, or pharmaceutical web properties carry substantial legal liability. Unconsented data sharing via pixels is now a primary focus of state enforcement and litigation.
- **Strict Bans on Geofencing:** Pioneered by states like Washington, Nevada, New York, and Connecticut, specific health privacy statutes explicitly prohibit setting virtual perimeters (typically ranging from 1,750 to 2,000 feet) around healthcare facilities to track or target patients. The 2026 regulatory shift was capped by major statutory enactments in California and Virginia. Effective

January 1, 2026, California's AB 45 explicitly outlawed geofencing around healthcare facilities for ad-targeting purposes, while Virginia's SB 338 (effective July 1, 2026) banned the commercial sale of precise geolocation data altogether. These law changes reflect a growing legislative push to eliminate location tracking, which regulators increasingly view as a proxy for revealing sensitive consumer behaviors – such as visits to healthcare facilities, reproductive health clinics, addiction recovery centers, and places of worship.

- **Mandatory Opt-In Consent:** Under modern state health statutes and FTC enforcement standards, passive consent mechanisms and bundled terms of service are legally insufficient. Except where data processing is strictly necessary to deliver a requested product or service, organizations must secure explicit, unbundled opt-in consent prior to collecting, sharing, or monetizing consumer health information.

2026 State and Federal Trends

As expected, the states have taken a patchwork approach when it comes to the sale of sensitive data. Since the close of the 2026 state legislative session, we have seen the following trends emerge:

- **Bans on the Sale of Sensitive Data:** In 2026, state legislatures increasingly moved toward outright prohibitions on the monetization and commercial transfer of sensitive consumer information. States including Delaware (HB 380), Maryland (MODPA), California (AB 1542), and New Jersey (A5328) instituted strict bans on sensitive data sales—with Maryland and New Jersey entirely eliminating standard opt-in consent carve-outs for monetizing non-HIPAA consumer health data, precise geolocation, and data about minors. Conversely, Virginia (S.B. 754) enacted a more targeted ban focused specifically on reproductive and sexual health data while leaving its broader sensitive data sale provisions open to statutory interpretation. This expanding patchwork of absolute sales prohibitions has severely disrupted third-party health audience segment availability and programmatic ad targeting across data broker networks.

- **Federal Legislation Watch:** It is crucial for healthcare marketers to track federal legislative proposals, including S.3097. Passage of this bill would mark a major pivot toward a HIPAA-aligned "Permitted Uses" framework, potentially creating a unified national baseline that streamlines today's state-by-state patchwork while creating new federal compliance obligations. Marketers should also keep a close eye on potential omnibus privacy measures, such as the SECURE Data Act.

The Californication of Health Data Privacy

California remained at the forefront of consumer health data privacy in 2026, preserving and expanding the nation's most rigorous legal framework. Through proactive rulemaking by state regulators and aggressive enforcement by the state attorney general, California established stringent compliance benchmarks that directly affect publishers, advertising technology platforms, and advertisers functioning across its market.

Highlighting this enforcement push, the California Attorney General announced a $1.55 million CCPA and UCL settlement with Healthline Media LLC on July 1, 2025. This action represented the largest CCPA penalty to date, as well as the first targeting a digital publisher and addressing health data. The Department of Justice's inquiry found that faulty opt-out mechanisms permitted behavioral advertising cookies to transfer sensitive medical inferences to third-party vendors. Attorney General Rob Bonta emphasized the state's resolve to use its statutory power against online tracking mechanisms to safeguard sensitive personal health information.

In parallel regulatory developments, the California Privacy Protection Agency (CPPA) finalized implementation rules for the DELETE Act on November 8, 2025, which came into force on January 1, 2026. These regulations introduced the Delete Request and Opt-out Platform (DROP), enabling individuals to submit centralized deletion requests to registered data brokers through a unified online portal. This framework substantially reshapes third-party data availability for advertising entities. Starting August 1, 2026, registered data brokers must query DROP every 45 days, purge corresponding consumer records – including health inferences – unless an exemption applies, convey request status updates within 45 days, and maintain documentation to prevent subsequent re-collection. For healthcare media buyers, this mandatory 45-day purge cycle triggers rapid audience segment decay across programmatic platforms, rendering static third-party health segments unsustainable and accelerating the shift toward contextual targeting and consented first-party data.

Even as these structural DROP requirements were rolling out, CalPrivacy signaled its immediate enforcement stance on health data broker oversight through a January 8, 2026 action against Rickenbacher Data LLC (d/b/a Datamasters).. The agency penalized the Texas-based information reseller for violating the Delete Act by buying and selling targeted advertising lists containing sensitive medical conditions—including Alzheimer's disease, drug addiction, and bladder

incontinence—without registering with the state. Beyond a $45,000 administrative fine, the stipulated order permanently barred Datamasters from selling personal information of California residents and mandated the complete deletion of previously acquired Californian data. This enforcement action established that CalPrivacy will utilize Delete Act violations not merely as a registry compliance mechanism, but to purge unauthorized health-data monetizers from the state marketplace entirely. For healthcare marketers, this precedent effectively dismantles the supply chain for off-the-shelf, condition-based audience segments across programmatic platforms. Consequently, agencies must enforce strict data provenance audits on ad-tech vendors while pivoting campaign strategies toward consented first-party data and contextual targeting.

Evolving Federal Approaches to Health Data Privacy

The federal policy landscape reflects an evolving dual strategy: combining strict oversight of non-HIPAA health data with targeted enforcement against deceptive commercial and lead-generation practices. Federal regulators during the Biden era initially established stringent baselines around sensitive consumer information through a series of landmark FTC actions—notably the $1.5 million *GoodRx* enforcement order and the $7.8 million *BetterHelp* settlement, followed by enforcement against *Cerebral* and *Monument*. These cases penalized digital health platforms for silently transmitting patient intake responses, mental health telemetry, and prescription interactions to ad networks like Meta, Snap, and Criteo.

Building on these cases, the FTC codified this enforcement doctrine by issuing its finalized Health Breach Notification Rule (HBNR). The updated HBNR explicitly expanded the definition of a "breach of security" beyond cyberattacks to include any unauthorized transmission of personal health records to third-party ad platforms via tracking pixels or APIs, while broadening coverage to virtually all direct-to-consumer health applications. However, following the 2024 judicial ruling in *AHA v. Becerra*—which struck down HHS OCR's attempt to classify basic IP address logging on unauthenticated public webpages as automatic Protected Health Information (PHI)—primary federal oversight of digital health ad tracking shifted squarely to the Federal Trade Commission under Section 5 of the FTC Act and the updated HBNR.

Under the FTC, federal enforcement expanded to address broader market misrepresentations, heavily targeting deceptive health lead generation and predatory insurance schemes. A primary example was the FTC's August 2025 $45 million settlement with lead-generator MediaAlpha for deceptively collecting

sensitive health inputs to feed third-party telemarketing networks. Concurrently, the agency intensified scrutiny on subscription billing traps and dark patterns across digital health platforms, culminating in the establishment of the dedicated FTC Healthcare Task Force in 2026.

Crucially, this focus on marketing transparency did not replace structural ad-tech scrutiny; rather, federal regulators merged the two. The landmark July 2026 joint lawsuit filed by the FTC, Utah, and California against Hims & Hers Health, Inc. demonstrated that transmitting user intake details and health interactions to platforms like Meta and Snap – via tracking pixels, server-side conversion APIs, or custom audience match lists – remains a severe statutory violation when paired with public promises of confidential care.

For healthcare ad strategists and agency executives, these overlapping federal priorities dictate a mandatory two-pronged compliance model. Marketers must maintain technical stack discipline – replacing unconsented client-side tracking tags with consent-gated, server-side architectures that scrub health-revealing metadata prior to ad-network transmission – while ensuring that top-of-funnel promotional claims, influencer messaging, and privacy disclosures precisely reflect underlying data practices.

Navigating Compliance: Strategic Recommendations for Healthcare Marketers

To navigate this fragmented regulatory environment and protect both agency and client brand reputation, 4As Health recommends that agency leaders, media buyers, ad-tech strategists, and compliance officers implement six core operational safeguards:

1. **Pivot Toward Contextual Placements & Consented First-Party Data**
   Shift media planning away from cross-site behavioral tracking and third-party health condition lists. Reallocate budgets toward high-intent contextual placements (running ads alongside relevant medical content) and build owned first-party datasets using transparent, affirmative opt-in collection experiences.

2. **Implement Consent-Gated, Server-Side Tagging Architecture**
   Conduct technical audits across all digital assets to catalog active tracking pixels, tags, software development kits (SDKs), and conversion APIs. Replace unconsented client-side tracking tags with consent-gated, server-side conversion architectures that actively scrub health-revealing metadata, IP addresses, search terms, and sensitive event parameters before transmitting data to ad platforms.

3. **Enforce Strict Vendor & Data Broker Due Diligence**
   Audit third-party data providers and programmatic vendors for verifiable consent lineage. Verify that any data broker supplying audience segments in California is actively registered under the Delete Act and compliant with 45-day DROP portal purge queries. Immediately cease purchasing off-the-shelf, condition-specific audience lists that lack explicit consumer consent.

4. **Dismantle Proximity Geofencing Around Healthcare Facilities**
   Immediately eliminate location-based virtual perimeters (typically 1,750 to 2,000 feet) drawn around physical care facilities, reproductive health clinics, hospitals, and pharmacies. Re-architect location campaigns to rely exclusively on coarsened, compliant geographic parameters, such as ZIP codes, cities, or Designated Market Areas (DMAs).

5. **Align Promotional Claims & Marketing Disclosures with Back-End Data Flows**
   Audit top-of-funnel creative, landing page messaging, and influencer briefs to ensure public assurances regarding "private," "confidential," or "discreet" care precisely match underlying ad-tech data practices. Misalignments

between public privacy promises and active backend tracking code create immediate regulatory exposure under Section 5 of the FTC Act and state consumer protection laws.

6. **Establish Cross-Functional SOPs & Consent Workflows with Clients**
   Work closely with client legal and compliance teams to establish standardized campaign specs across target jurisdictions. Implement unbundled, affirmative opt-in consent mechanisms prior to media execution, ensuring that secondary data processing—such as ad targeting or performance analytics—is distinctly authorized by the consumer.

4As Health will continue to monitor state and federal health data privacy developments, providing our member agencies with the advocacy, guidance, and tools needed to lead in a consumer-first, privacy-safe healthcare ecosystem. A special thank you to Amanda Anderson, 4As Vice President for Government Relations, for her input and enhancements to this report.

Need Guidance?

For questions regarding state health privacy laws, ad-tech compliance, or 4As Health policy initiatives, reach out to **Rachel Kessler**, Manager, Government Relations: rkessler@4as.org or **Jim Potter**, Executive Director, 4As Health: jpotter@4as.org.