SQUIRE PATTON BOGGS

Health (and Health-ish) Data and Advertising Under Scrutiny

US – June 2023

In 2020, when the California Consumer Privacy Act (CCPA) came into effect, the privacy landscape in the US changed forever. Fast forward three years, we now have close to a dozen states that have passed consumer privacy laws, with the second generation of consumer privacy laws giving particular attention to sensitive data.

In particular, there is an emerging trend, in both new legislation and enforcement of existing privacy and consumer protection regimes, towards a focus on the collection, use, and sharing or selling of health-related personal information, specifically information that is outside the scope of the federal Health Insurance Portability and Accountability Act (HIPAA).[1]

The effect is a restriction on what publishers, advertisers, and other commercial enterprises can do with consumer health information, often broadly defined to include any past, present or future health status or inference regardless of sensitivity (e.g., acne or a headache). These developments include:

- As of July 1, 2023, privacy regulators in four states – California, Colorado, Connecticut, and Virginia – require, and will have the ability to inspect, data protection assessments of processing of consumer health information and other sensitive data, and these states' laws will require opt-in or opt-out of uses for advertising and certain other purposes.

Also in July of this year, companies that carry out geofencing near medical and similar facilities will have to comply with Washington's My Health My Data (MHMD) law and New York's recently passed law – and simply must stop doing it in those states, subject to very limited exceptions. Connecticut and Nevada have passed similar laws, which are pending their respective governors' signatures. If signed by the governor, the consumer health information portions of Connecticut's version of MHMD will go into effect in July of this year.

In March 2024, the remainder of MHMD comes into effect, requiring complex notice and consent requirements for collection, use, and/or sharing or selling of consumer health information beyond what is necessary to provide requested services, such as for advertising, and notice and other protections even for purposes of providing requested services. If signed by the governor, Nevada's health-specific privacy law that was inspired by MHMD will become effective on March 31, 2024.

Other states are sure to follow, and the Federal Trade Commission (FTC) is using its authority under the Health Breach Notification Rule (HBNR) to restrict secondary uses of consumer health information by digital health apps and others that fall within the scope of that rule.

As a result, businesses that are not HIPAA-regulated healthcare providers, but that handle consumer health information, will need to choose between (1) providing differential privacy practices dependent on residency (where possible), including user experiences (e.g., type of notice and nature of consent) on the front end and heightened privacy protections on the back end, or (2) adopting a high watermark approach that applies the strictest restrictions and obligations by default to all users.

Particular attention should be given to the use of consumer health information for targeted advertising as these laws, and potentially implications from recent enforcement action settlements, diverge from ad industry self-regulatory programs, mandate higher consent requirements, and outright prohibit certain location-aware health related advertising.

In view of this increased legislative, regulatory, and enforcement attention and activity, your business should:

- Not discount the potential relevance of these developments to your organization. These legislative and regulatory schemes covering consumer health information apply more broadly than to just healthcare and healthcare-adjacent organizations.
- Start educating your organization's stakeholders on these issues now. The effects of these laws, particularly MHMD and its progeny, will be ground shifting. This is not business as usual. Many organizations handling consumer health information should be prepared to make changes to address evolving obligations and restrictions.
- Continue – or start – to audit your company's consumer health information use cases. This includes applying the state consumer privacy laws in California, Colorado, Connecticut and Virginia; the FTC's Health Breach Notification Rule; and finally, the Washington, New York, Nevada and Connecticut health-specific privacy laws. Under the state consumer privacy laws, your company is likely required by July 1 of this year to carry out data protection impact assessments/risk assessments with respect to use cases involving consumer health information. This process should look beyond what is required by those laws of general application, and also to health-specific laws and regulatory enforcement positions being advanced by state and federal consumer protection authorities.

1 We refer to this type of personal data that is unregulated by HIPAA as "consumer health information." Notably, different definitions are given to this type of data depending upon the regulatory regime.

- Address your existing and impending obligations. This includes:
  - Notice and consent/authorization and/or opt-out requirements
  - Privacy policies and notices
  - Data protection impact assessments/risk assessments
  - Vendor and third-party management (including contract remediation)
  - Data security assessments and remediation
- Understand your organization's risk posture and, if desired and/or necessary, technical and operational ability to provide differential privacy practices to residents of different states, or avoid collection and processing of consumer health information of certain states' residents for restricted purposes.
- Even for residents in states that do not have laws regarding consumer health information, confirm that your activities do not bring you within the scope of the HBNR, which will capture many non-HIPAA-regulated digital health products and services, and beware of practices that could be deemed deceptive or unfair, keeping in mind that health-related data will be treated as sensitive, and therefore deserving of heightened protection.

Summary of Regulatory, Legislative, and Enforcement Activity

FTC Action

The FTC, on the heels of a 2021 policy statement on health mobile apps and 2022 updates made to the FTC's interactive tool and best practices guidance for businesses creating and marketing mobile health apps, issued three high-profile orders (*GoodRx*, *BetterHelp*, and *Premom*) involving alleged violations of deceptive and unfair activities under Section 5 of the FTC Act and, in some cases, violation of HBNR. These orders, while they are merely settlements of claims brought under a number of theories, including allegations of deception, and are not rulemakings, suggest that the FTC expects businesses to obtain consent for the use of consumer health information for ancillary purposes, such as targeted advertising, and otherwise clarifies when a digital health application needs consent to share data. In particular, the unfairness claims, and the treatment of consumer health information as highly sensitive, lay the foundation for a consent-based standard even without specific federal statutory or regulatory obligations, such as is the case when the HBNR applies (e.g., mobile apps collecting consumer health information from multiple sources).

Following these orders, in mid-May, the FTC proposed amendments to the HBNR that seek to clarify business's obligations and broaden the scope of the rule, and is seeking public comments on the proposals. All signs point to the FTC's desire and intent to codify its 2021 policy statement into the HBNR.

The amendments include:

- Revising and adding definitions to clarify how the rule applies to health apps and similar technologies, and what it means to draw data from multiple sources (the trigger for the rule's applicability).
- Redefining breach of security to clarify that it includes an unauthorized acquisition of identifiable health information that occurs as result of an unauthorized disclosure. This merely codifies the FTC's current interpretation that unauthorized acquisition includes both data breaches and unauthorized disclosures.
- Expanding the content required in notices, and providing exemplar notices.

A day before the *BetterHelp* settlement announcement, a trio of FTC commissioners issued a joint statement expressing concern about the sale of membership-based primary care practice One Medical. The letter warns that "Since announcing the proposed acquisition, [the buyer and the seller] have expressly represented to the public that they will not share consumers' 'personal health information' for advertising or marketing purposes without their clear permission. The statements in One Medical's privacy policies, combined with the recent public statements by both companies about privacy, constitute promises to consumers about the collection and use of their data by the post-acquisition entity."

State Health Data-specific Laws

- **Washington** – Spurred by the US Supreme Court's invalidation of *Roe v. Wade* in the *Dobbs* case, Washington State passed MHMD, with some portions of the law becoming effective in July 2023 and others in March 2024. MHMD regulates health and health-adjacent activities far beyond protecting access to reproductive health and gender-affirming care, and, in part due to the private right of action and broad extraterritorial reach, will likely prove to be a ground-shifting piece of legislation that will require many businesses to change the way that they do business unless the law is narrowed through amendments.
- **New York** – The State of New York has followed suit and enacted several new laws designed to protect electronic consumer health information and prevent unauthorized disclosure, most notably banning geofencing around any health care facility, by anyone other than that facility, for the purpose of sending ads, building consumer profiles, or inferring consumer health status.
- **Connecticut** – As of July of this year, Connecticut's consumer privacy law requires opt-in consent to secondary uses of sensitive data, including personal data revealing a health condition or diagnosis. Recent amendments to that law will require, as of July 1, more stringent notice and consent requirements for collection and/or sharing or selling of consumer health information, and a ban on geofencing healthcare facilities.
- **Nevada** – In March of 2024, Nevada's new health-specific privacy legislation will ban the geofencing of healthcare facilities for purposes of identifying, tracking, collecting data from or sending messages to consumers, and implement strict notice and consent requirements for collection and/or sharing or selling of consumer health information.

State Consumer Privacy Laws

- As of January 1, the CCPA (as amended by ballot initiative) and Virginia Consumer Data Privacy Act (VCDPA), and their provisions regulating sensitive personal information/data, came into effect. The CCPA provides the right to limit use and disclosure of sensitive personal information, while the VCDPA requires consent for any collection or other processing of sensitive personal data, with both laws including certain health data as sensitive, subject to various exceptions such as providing requested services.[2]
- The Colorado Privacy Act's rules were finalized on March 15 and have fleshed out consent requirements that apply to sensitive data – which includes "a mental or physical health condition or diagnosis" – and added detailed rules on sensitive data inferences and secondary uses of personal data. The law is effective as of July 1. Connecticut's privacy law, which also regulates certain health data, also becomes effective on July 1 and, as noted above, recently expanded its requirements for consumer health information.
- As of the date of this post, five state legislatures passed consumer privacy laws during this year's legislative session – Florida, Indiana, Iowa, Montana, Tennessee and Texas – adding to the list of state laws that will require either an opt-out or opt-in consent for the processing of consumer health information.

State Consumer Protection Activity

- Mirroring the FTC, attorneys general across the country also have expressed concerns about consumer health information, particularly when used in the context of so-called corporate surveillance, the term used by President Biden and the FTC to describe personalization and targeting of advertising.
- Late last year, thirty-three attorneys general – led by then Attorney General (now Governor) Maura Healy of Massachusetts – wrote a letter to the FTC sharing their concerns about consumer health information, noting that it is "particularly sensitive, as it can be combined with other information to reveal intensely personal information."

Also, at the state level, several lawsuits allege violations of state consumer protection laws due to unauthorized use of consumer health information and HIPAA protected health information (PHI) collected via portals used by patients to communicate with healthcare providers for targeted advertising purposes. (See our related post for more detail.)

Do Not Forget HIPAA

So far, we have focused on non-HIPAA data. HIPAA is a federal law that regulates "covered entities" and "business associates" when they receive or create PHI. As Privacy World previously reported, the US Department of Health and Human Services' Office for Civil Rights (OCR), HIPAA's primary enforcement authority, is looking at digital advertising and other data practices of the entities it regulates. OCR published a bulletin requiring HIPAA-regulated entities to undertake fact-based analyses to determine whether and when tracking technology deployed on their websites (e.g., cookies) and mobile apps complies with HIPAA. On information and belief, OCR has several ongoing investigations into use of pixels and cookies on the online services offered by covered entities, and a slew of class action litigation has been brought against healthcare providers alleging that online services' tracking technologies are sharing their PHI with social media platforms, adtech providers and others without data subject consent, in violation of HIPAA and state tort laws.

Conclusion

These recent FTC settlements, coupled with state law developments, should prompt businesses to consider:

- What consumer health information is collected, used or disclosed, and for what purposes?
- When is consent, and what type of notice and consent, necessary for desired uses?
- What third parties may have access to consumer health information and what can reasonably be done to prevent, and to take action in the event of, an appropriate access or use?
- What consumer rights (e.g., access, correction, deletion, opt-in/out, limit-the-use, etc.) are applicable?

In order to meaningfully do so, companies need to implement a data protection risk and impact assessment program, which includes special attention to consumer health information. To learn more about conducting data practice assessments see Navigating Data Privacy Assessments Amid New State Laws.

For more information, contact the authors or your relationship partner at the firm.

2 The VCDPA's definition is limited in that it defines "mental or physical health diagnosis" as sensitive data, while the CCPA regulates as sensitive personal information "personal information collected and analyzed concerning a consumer's health."

Contacts

Alan Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Kyle Fath
Partner, Los Angeles/New York
T +1 212 872 9832
E kyle.fath@squirepb.com

Kyle Dull
Senior Associate, New York/Miami
T +1 212 872 9863
E kyle.dull@squirepb.com

Gicel Tomimbang
Associate, Los Angeles
T +1 305 577 2840
E gicel.tomimbang@squirepb.com