LOEB & LOEB LLP

Understanding the Health Regulatory Triangle through Pixels — HIPAA, FTC's Breach Notification Rule, and State Privacy Regulations

Eric Cook CIPP/US

Client Alerts/Reports October 2023

Hashed & Salted | A Privacy and Data Security Update

The use of online tracking technologies such as pixels, software developer kits (SDKs) and cookies to better understand users' behavior on a business's websites and mobile applications was intended to be a simple endeavor; however, the recent deluge of class-action lawsuits as well as federal and state privacy enforcement and regulations is certainly complicating many businesses' efforts to reach their consumers online. In the past six months alone, these settlements have been announced:

- Advocate Aurora for $12.25 million
- GoodRx for $1.5 million
- BetterHelp for $7.8 million
- Premom for $100,000
- Vitagene for $75,000

There also has been continuing litigation throughout the country concerning the use of tracking technologies and potential violations of the Video Privacy Protection Act (VPPA), federal and state wiretapping laws, and common law privacy rights.

In addition to the above settlements and litigation, the Federal Trade Commission (FTC) and the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) have issued joint guidance and notices to hospitals, telehealth providers and other digital health companies concerning potential violations of both the Health Insurance Portability and Accountability Act (HIPAA) and the FTC's Health Breach Notification Rule (HBNR) as well as Section 5 of the FTC Act. As a result, many businesses and their service providers typically not regulated under these laws are intensely focused on whether recent interpretations by the OCR and the FTC under both HIPAA and the HBNR apply to their businesses. Furthermore, these same businesses are engaging in compliance activities concerning both comprehensive state privacy regulations, such as the California Consumer Privacy Act (CCPA), the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act, (CDPA) and state-specific health privacy laws, such as Washington's My Health My Data Act (MHMD) and Nevada's act, to name just a few.

Businesses may have originally taken the wait-and-see approach in response to the FTC's previous guidance concerning the collection, use and disclosure of health data; unfortunately, this approach is no longer tenable for businesses, whether regulated by the FTC, HHS or any one of the various state privacy laws, when they collect personal information that may actually qualify as sensitive health data. In addition to announcing this year four settlements concerning health data, the FTC recently concluded its public comment period concerning its proposed changes to the HBNR, which are consistent with the FTC's current interpretation regarding what entities and health data are subject to the HBNR. Under the proposed changes, the FTC will strengthen its enforcement powers, as it would clarify that the HBNR would apply to most health and wellness apps as well as treating the unauthorized disclosure of consumer health data as a breach, including the disclosure of consumers' health data through tracking technologies such as pixels without the consumers' consent. Furthermore, three states—Washington, Nevada and Connecticut—have passed state-specific health privacy laws, with Washington passing the most prescriptive regulation of the three. Finally, roughly a dozen comprehensive state privacy laws have passed that regulate health data as sensitive data requiring enhanced opt-in or opt-out protections and data impact assessments.

What Do You Need To Know?

- What has changed with HIPAA?
- Is the FTC's stance on health data any different from HHS?

What has changed with HIPAA?

Since our last article, the HHS OCR issued a bulletin that asserts that personal information—including but not limited to internet provider (IP) address, email address and dates of appointments—when collected from a hospital's authenticated website (e.g., patient portal) in and of itself would be treated as personal health information (PHI) under HIPAA regardless of whether the consumer has a preexisting relationship with the hospital. In some instances, when a consumer has not entered credentials but their actions on a covered entity's webpage are being observed through pixels, cookies, heat maps and other tracking technologies that provide data (e.g., IP address or email) concerning an individual's interest in a treatment or condition, their data may be treated as PHI when it corresponds to an identifiable individual. Consequently, covered entities may disclose PHI collected from their websites or mobile applications only for "permissible" or "required" purposes. Under HIPAA, permissible purposes include using PHI for treatment, payment and health care operations. Required purposes includes disclosures to the individual and to HHS. However, disclosures for marketing purposes are not considered permissible and thus require individual authorization under HIPAA. Furthermore, OCR has stated, "[T]he disclosure of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliance authorizations, would constitute impermissible disclosures" under HIPAA.

Additional HIPAA implications:

- For covered entities such as hospitals, HHS' interpretation may mean that businesses (e.g., mobile developers, agencies) will become business associates to the extent they provide services concerning a regulated function or activity (e.g., consulting, management) under HIPAA and create, receive or maintain PHI in order to provide their products and services.

- For business associates such as agencies, mobile app developers and service providers, HHS' interpretation may mean not only that these businesses become business associates of their hospital clients, requiring them to now comply with the HIPAA security rule, but

that the business associate may now have to comply with additional HIPAA requirements under its business associate agreement with the hospital. In addition, these businesses are required to enter into a business associate agreement with their subcontractors that assist in providing services to the hospital for the covered function or activity.

- Finally, covered entities will be required to obtain HIPAA-compliant authorizations from individuals to the extent that their collection and disclosure of PHI are not carried out for health care operations and they would like to use this information for marketing purposes. Cookie banners will not be sufficient to obtain a HIPAA-compliant authorization from individuals.

As a result of the heightened bar, the collection of information from websites and/or mobile applications likely have higher risks to the extent that they require a consumer to enter credentials (i.e., authentication) and that the data collected can be attributed to a reasonably identifiable individual. Finally, where HIPAA does not apply, the FTC has signaled that it has no problem stepping in to enforce.

Is the FTC's stance on health data any different from HHS?

To a certain extent, the FTC and HHS have maintained a similar stance on health data. Information collected from a sensitive website that can be attributed to an identified or identifiable individual is sensitive health data that will be regulated. As a refresher, the FTC's HBNR applies to businesses to the extent they are not covered by HIPAA, and applies specifically to "vendors of personal health records." Whether a business is subject to HIPAA versus the HBNR basically hinges on whether the product or service is being used or supplied at the direction of a covered entity or the consumer. If the product or service is controlled and/or directed by the consumer, the business likely falls under the HBNR. However, as we have seen with recent regulations, entities can be subject to HIPAA for parts of their business while subject to HBNR for other portions.

What are the most important takeaways from the FTC's recent enforcement of health data rules?

The FTC intends to use all of its enforcement tools to regulate the use of sensitive health data by small and large businesses to the extent they are not regulated by HIPAA. Most importantly, information collected from sensitive websites and mobile applications will be treated as sensitive health data to the extent that it is identifiable information. The FTC has treated the collection of information from prescription, mental health, ovulation tracking and genetic apps as sensitive health data that will be protected. And it will use both its HBNR and Section 5 powers to prohibit the disclosure of sensitive health data without notice and proper consent from consumers. In addition, businesses

should have policies and procedures internally that align with their external privacy notices to consumers concerning how they handle sensitive health data.

As an example, the FTC's first enforcement action under the HBNR was levied against GoodRx for a $1.5 million fine. In addition to violations of the HBNR, the FTC complaint alleged that GoodRx violated Section 5 of the FTC Act when it violated its own privacy statements to consumers, which stated hat it would not share personal health information with third parties, including advertisers, and thus engaged in "unfair or deceptive acts or practice, in or affecting commerce." Furthermore, GoodRx was alleged to be subject to the HBNR as a vendor of personal health records when it failed to notify consumers, the FTC and media after disclosing individually identifiable health information to third parties without consumers' consent—and thus without authorization—in violation of the HBNR. Notably, in addition to paying $1.5 million in civil penalties, the FTC's order requires that GoodRx must:

- Not share health data for advertising at all
- Implement a comprehensive privacy program to protect consumer health data
- Obtain affirmative express consent before disclosing user health information to any third party for any other purpose

Interestingly, the FTC treated GoodRx, unlike BetterHelp, as a "vendor of personal health records" and enforcement was not limited to the FTC's Section 5 powers, arguably because GoodRx collected data not only from consumers' inputs but also from health data pulled or capable of being pulled from pharmacy benefit managers. While the remedies in each case are specific to the facts and the parties at issue, they do shed light on the FTC's positions. For example, we know the FTC expects companies to get affirmative express consent prior to disclosing individually identifiable health information to third parties for advertising purposes. Business should also be aware that violations under the FTC's authority could result in fines up to $43,792 per violation per day. However, in addition to civil penalties under the HBNR, businesses must also manage the potential risks of enforcement by state attorney generals and, in the case of Washington's MHMD, individuals.

What can MHMD teach us about health-specific state regulations?

As of now, three states—Washington, Connecticut and Nevada—have passed health-specific state privacy regulations intended to provide enhanced protections for consumers' health data. Here we will focus on Washington's MHMD as the strictest standard. You can review our

State Health Data Comparison Chart to see how these laws compare.

First, MHMD has broad applicability, as it applies to entities that conduct business in Washington or produce or provide products or services that are targeted at consumers in Washington and "alone or jointly with others determines the purposes and means of collecting, processing, sharing, or selling consumer health data." For most companies that operate online or via mobile apps, MHMD will apply to their Washington-based consumers. Likewise, MHMD will apply to all vendors, including service providers and third parties, to the extent they jointly assist clients subject to this law with services such as implementing pixels for marketing purposes. In addition, MHMD defines consumer health data as personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future mental health status. This definition is also broad and includes any identifiable information such as IP address, search terms and other user behaviors that are attributable to an identifiable individual and may relay their past, present or future mental health status. Thus, an IP address or mobile advertising ID associated with a certain advertising segment to market-sensitive products or services may be considered consumer health data. Finally, unlike the Nevada and Connecticut laws, MHMD provides consumers with the ability to bring legal action against regulated businesses in their individual capacity. Furthermore, MHMD provides certain exemptions for health data; however, these exemptions are limited specifically to certain data such as PHI under HIPAA and do not extend to the entities themselves. As a result, regulated businesses must:

- Provide a consumer-specific health privacy policy
- Enter into data-processing agreements with vendors with certain obligations and restrictions concerning consumer health data
- Not engage in the sale of consumer's health data without signed, written authorization

In addition, regulated business will want to pay particular attention to the fact that the definition of consumer health data under MHMD is not limited to health data but includes non-health information, including proxy, derivate, inferred or emergent data created by any means, including machine learning or algorithms. These health-specific privacy laws do create enhanced obligations surrounding consumer health data but unfortunately are not the end of the analysis concerning a business's obligations when using health data.

Comprehensive state privacy regulations

All of the 12 comprehensive state privacy regulations that have been passed to date in some way regulate the use and disclosure of health data. California, Virginia, Colorado, Connecticut, Utah, Iowa, Montana, Texas, Indiana, Tennessee, Oregon and Delaware comprehensive state privacy regulations all regulate health data to the extent it reveals information about an individual's mental or physical health condition or diagnosis. Of the states referenced, Virginia, Colorado, Connecticut, Montana, Texas, Oregon, Tennessee, Indiana and Delaware require consumers to opt in before their sensitive health data may be used by businesses, while California, Utah and Iowa require consumers to opt out of the use of their sensitive health data. For instructive purposes, we will focus our discussion on the potential implications of using tracking technologies when a business is subject to the CPA. The collection of personal data that reveals the physical or mental health condition or diagnosis of an individual under the CPA is treated as sensitive data and requires the controller to obtain opt-in consent before processing such data and to conduct a data protection assessment.

Ultimately, with so many land mines existing in this current environment, it is very important that all businesses assess whether they are creating, accessing or maintaining sensitive health data as defined under the guidance, enforcement and regulations or are providing products or services to a client or customer that does.

What Should We Do Now?

Businesses should start by assessing their activities to determine whether and in what context these changes will impact their business. Businesses should be answering the questions:

a. What laws apply to you? View Health Data Decision Tree

b. Does your business use tracking technologies such as pixels, cookies or SDKs for its websites or mobile applications or implement such technologies for its clients?

c. If so, are these technologies used on websites or mobile applications of any business providing medical or health-related services, including medical treatment, medical payment, mental health, genetic testing, gender-affirming care, prescription services, telehealth or women's health?

d. Does your business implement and use these technologies on any website or mobile applications that might be considered sensitive to consumers generally? Sensitivity is obviously subjective, but consider whether someone would be embarrassed or subject to emotional distress if the use of the website or app (e.g., a website with information on sexual identity or reproductive health) were revealed.

e. Where else could your business collect or receive information that falls within the definitions of health information under the laws that apply to you?

f. Does your business or client qualify as a covered entity or a business associate under HIPAA?

g. If you are a business associate, does your business provide marketing services to a covered entity?

h. Do you know what states your consumers reside in? Consider whether you can limit the scope of these laws to your consumers in the relevant states or whether you will apply the rights and obligations across all consumers.

Next Steps:

✓ Conduct a data inventory of the health data your business collects, creates, accesses or maintains itself or on behalf of its clients (e.g., hospital, pharmaceutical company, etc.).

✓ Conduct a risk analysis under HIPAA or a data impact assessment under state privacy laws.

✓ Update vendor agreements to specifically restrict what your vendors can do with health data and to determine whether you need to (and can) shift the allocation of risk.

✓ Discuss the feasibility of an audit process for vendors handling sensitive personal information.

✓ Align internal practices with your external privacy policies and statements. Create a cadence of review to ensure information does not become outdated.

✓ Make sure your business has properly configured any pixels, SDKs and cookies so that they are operating consistent with your privacy notices.

✓ Design a cadence for review of new pixels, SDKs and similar technologies to confirm that your program remains in compliance.

✓ Consider the form and language of consumer authorizations in the event you decide to obtain consent.

If your business has any questions in response to going through the above exercise, do not hesitate to reach out to our Privacy, Security & Data Innovations team here at Loeb.
Click here to download a PDF of the full alert.

RELATED SERVICES

Privacy, Security & Data Innovations

RELATED PROFESSIONAL

Eric Cook CIPP/US

Associate

+1.312.464.3187 ecook@loeb.com