The FTC to Digital Health Companies: Think Twice (or Thrice) About Your Privacy Practices

02-08-24 • alert • katherine leibowitz

The privacy of consumer health information suffers from a serious coverage gap. Unlike the European Union, the United States has no comprehensive data protection law at the federal level. HIPAA[1] is sector-specific. To help fill this gap, over the past fourteen months, two government agencies have made headlines with their consumer health data privacy initiatives. We explore those here, focusing on the impact for digital health technologies and entities covered by HIPAA.

Section I: Setting the Stage

In 2018, California passed the groundbreaking state consumer privacy legislation (CCPA [2], amended by the CPRA[3]) modeled on the European Union's General Data Protection Regulation (GDPR). For several years, companies adjusted to the rigors of GDPR and California law (with some hoping to avoid applicability altogether). Then a number of states joined the fray, creating a labyrinth of regulatory requirements, to the endless frustration of company compliance officers. [4]

Combined with this sparse federal landscape of data protection law is the recent explosion of digital health technologies such as mobile health apps, wearables and related software as a service (SaaS). While revolutionizing healthcare, these technologies highlight the limited scope of HIPAA and the patchwork of state laws. Depending on the context, the same information may or may not be regulated by one or more of these laws. Last year, the consumer watchdog agency known as the Federal Trade Commission (FTC) released its Baker's Dozen, took high profile enforcement actions, and teamed up with HHS OCR[5] to shore up the handling of consumer health data.

Companies sorting through the various state privacy laws (which is beyond the scope of this post) should heed the federal enforcement environment, particularly at the FTC level. This post walks through recent FTC and OCR activity and delves into the best practices reflected in the FTC's Baker's Dozen. We wrap up with next steps for your compliance department.

Section II: HIPAA, Section 5 of the FTC Act, and the HBNR

The three primary tools that the FTC and HHS OCR use in their pursuit of data protection are HIPAA, Section 5 of the FTC Act, and the Health Breach Notification Rule (HBNR). Digital health companies and entities covered by HIPAA need to pay careful attention to the interplay among the three. The FTC published an in-depth post about this in September 2023.

II.A: HIPAA

HIPAA applies to "covered entities" and "business associates."

- Covered entities are (1) health plans, (2) health care clearinghouses, and (3) health care providers that conduct standard healthcare transactions electronically.
- "Business associates" perform services involving protected health information (PHI) on behalf of or to covered entities.[6]
- In many instances, HIPAA requires an individual's authorization for the use and disclosure of their PHI. Information that is de-identified per HIPAA's requirements is not considered PHI. However, many entities that deal with personal health data are beyond the reach of HIPAA. This is where the FTC comes in.

II.B: Section 5 of the FTC Act and HBNR

The FTC has two primary enforcement tools: Section 5 of the FTC Act and the HBNR. Any enterprise collecting personal data, whether or not health-related, is subject to the FTC's jurisdiction.

- Section 5 of the FTC Act is aimed at preventing "unfair" and "deceptive" business practices. This includes deceptive or misleading claims to consumers about the collection, use, and disclosure of their own health information. An entity can be subject to both Section 5 of the FTC Act and HIPAA.
- The HBNR applies to certain businesses that are not covered by HIPAA, including vendors of personal health records (PHR), PHR-related entities and third party service providers. An FTC Policy Statement indicates that makers of health apps, connected devices and similar products must comply with the HBNR. Last year, the FTC proposed changes to to the HBNR to clarify the rule's applicability to health apps, fitness trackers, wearables and similar technologies. Of note, in addition to the more routine concept of data security breach, an "unauthorized disclosure" by a company – such as sharing data with advertisers through tracking technologies – could qualify as a breach under the HBNR and would require notification to affected consumers, the FTC, and in certain cases, the media.

Section III: Recent HHS OCR and FTC Activity

HHS Bulletin:

- In December 2022, HHS OCR issued a bulletin aimed at the use of tracking technologies by HIPAA covered entities and business associates on their websites and mobile apps. The bulletin states, "Regulated entities are not permitted to use tracking technologies that would result in impermissible disclosures of protected health information (PHI) to tracking technology vendors." OCR explains, "For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."
- In plain English, web tracking technologies that link a visitor's IP address with their browsing of the hospital's (or other covered entity's) public web site pages violates HIPAA unless proper authorization was first obtained. As further explained below, industry is challenging this bulletin as an overstepping of OCR's authority.

FTC Enforcement Actions:

- In the Spring of 2023, the FTC brought several high-profile enforcement actions against companies offering digital health platforms and mobile apps, including GoodRx, BetterHelp, Premom, and Vitagene. These enforcement actions highlight how seriously the FTC is taking the disclosure of consumer health data and reflect a laser focus on (a) data shared for advertising purposes, (b) company privacy policies, and (c) insufficient securing of data.
- The penalties include banning companies from disclosing health data for advertising purposes, monetary penalties totaling almost $9.5 million, civil penalties, data and algorithm deletion, and holding individuals personally liable for their company's security.

Class Actions:

- Government enforcement actions often go hand in hand with civil litigation.
- Following on the heels of the FTC enforcement action, in November 2023, GoodRx agreed to settle a class action lawsuit for $13 million. The plaintiffs had alleged unauthorized (i.e., without their consent) disclosure of their personal health information via tracking technologies.
- The recent government activity relating to tracking technologies has also spawned data privacy class action lawsuits against Meta, Google and others for pixel tracking.

FTC OCR Joint Letter:

- In July 2023, the FTC and HHS OCR teamed up to send a joint letter to 130 hospital systems and telehealth providers warning them of the risks involved in their use of online tracking technologies, such as pixels, to track consumer activity. The letter provides a nice outline of the differences in coverage and function of HIPAA, enforced by HHS, and Section 5 of the FTC Act and HBNR, enforced by the FTC.

Lawsuit Against OCR:

- Meanwhile, in November 2023, the American Hospital Association and others sued HHS OCR to challenge the December 2022 bulletin restricting the use of third-party tracking technologies, arguing that the restrictions negatively impact both hospitals and the public, and reflect an overbroad conception of PHI that exceeds OCR's authority under the HIPAA statute.

FTC Baker's Dozen:

- In July 2023, the FTC published the blog post, "Protecting the privacy of health information: A baker's dozen takeaways from FTC cases." Commonly referred to as the "Baker's Dozen," this post provides 12 key takeaways for companies collecting or using health data.
- We walk through the takeaways below. As the FTC says, "listen up."

Section IV: FTC's Baker's Dozen

If your company collects, uses, or shares personal health data, follow these best practices:

1) Health Information Includes More than You Might Expect:

- Beware of what constitutes health information. From the FTC's viewpoint, it includes what we typically think of as health information (e.g. medications, diagnoses) as well as anything that "enables an inference" about a consumer's health. This echoes the Washington State law.[7]
- What can enable inferences? As examples, the FTC mentions both the fact of a consumer using a health-related app or website (e.g. mental health or fertility) and how consumers interact withan app, such as turning on or off "pregnancy mode."

2) Employ Privacy-by-Design:

- Interweave your technology decisions with privacy considerations. GoodRx's and BetterHelp's failure to implement robust privacy policies and procedures contributed to the FTC's enforcement actions for unfair and deceptive business practices.

3) Use Pixel Tracking Technologies with Caution:

- The use of behind-the-scenes tracking technologies like pixels needs to be consistent with privacy policies and statements to consumers.
- If your use of tracking technologies results in data disclosure without consumers' express affirmative consent, this may violate Section 5 of the FTC Act and the HBNR. The GoodRx and Premom enforcement actions highlight this.

4) Data Recipients Can Also Get into Trouble:

- Both disclosing and receiving consumer health information create privacy obligations.
- Recipients need to conduct due diligence on their data providers to make sure the data provider has adequate rights to collect, disclose and transfer the data to the recipient for the purposes the recipient intends.
- Data recipients should be wary of standard contract terms used by data providers when collecting consumer health data. The FTC highlights marketing and advertising as a particular concern.

5) Coordinate Your Privacy Practices with Your IT and Compliance Departments:

- Your IT and compliance departments must coordinate with each other on the company's privacy practices, and to do that, you need to understand the data flow.
- Ensure communication among all departments and staff that handle data.
- Map all data flow, use and subsequent disclosure (see Next Steps below). Reflect this in your privacy policies. Otherwise, you risk violating your privacy policies from the start, and by now, hopefully we all know that violating your own privacy policy can land you in FTC hot water.

6) Don't say "HIPAA Compliant" or "HIPAA Secure" in a Deceptive Manner:

- To stay off of the FTC's radar, don't claim to be HIPAA compliant when you are not. And don't claim to be HIPAA compliant if your company is not actually covered by HIPAA.
- Keep in mind that only OCR can determine if a company is compliant with HIPAA.

7) HIPAA Seals and Certifications May Be Deceptive:

- Be wary of companies that offer HIPAA compliance certifications and seals. "If a company provides a health-related seal or certification to others that falsely implies that the recipient is covered by HIPAA, is complying with HIPAA, has been reviewed by a government agency, or has received government approval, both the certifier and the user of that false certification could be subject to FTC enforcement action." In other words, the FTC may go after both your company and the sealing company.

8) Retroactive Changes to Data Collected Under a Privacy Policy Followed by Continued Use Does Not Constitute "Consent":

- The common practice of reserving, in your privacy policy, the right to make changes to your privacy practices such that the visitor's continued use of the website/service constitutes consent to the changes may land your company in hot water.
- Vitagene clarifies that continued use does not constitute consent to material retroactive privacy policy changes (e.g., changes in practices regarding health data previously collected). Retroactively implementing material changes can constitute unfair practices.
- Notice and opt-in is the way to go, as opposed to the common practice of no choice or opt-out when updating a privacy policy.

9) Don't Hide Behind Ambiguous or Dense Privacy Policies or Terms of Service

- Avoid euphemisms and hiding the ball. Failure to use clear language can be unfair or deceptive.
- Use plain language and lay all your cards on the table. If express consumer consent is required (uniformly required by the FTC's recent health privacy enforcement cases), you must clearly and conspicuously disclose all material facts.

10) You May Be Liable Both for What You Say and What You Fail to Say:

- BetterHelp demonstrates that you can deceive consumers without making affirmative statements, such as by not disclosing material information about the use and disclosure of health information.
- Further, BetterHelp, Premom, and GoodRx all illustrate that if your practices harm consumers, your company can face FTC enforcement actions "regardless of who said what."

11) Companies Handling Biometric Data Must Be Particularly Security-Vigilant

- Biometric data such as voice data, video data, and DNA information is particularly sensitive. Security failures regarding this category of data will be a priority for FTC

moving forward.

12) Reproductive Privacy Is a Special Priority for the FTC:

- FTC actions against Premom and Flo, and guidance on reproductive privacy (among other things) reflect this top area of concern.

Section V: Next Steps for Industry

The following four points are fundamental to your compliance department's implementation of the Baker's Dozen, HIPAA compliance (if applicable) and the growing body of state privacy laws:

1) Data Mapping:

- Document what types of data your entity handles. For each data type, identify where the data is stored, how it is used, with whom it is shared (or accessible by), for what purposes it is shared (or accessible by), and which laws or regulations apply.

2) Technology Mapping:

- Determine what tracking technologies are used on your websites, apps and any other digital interfaces, how the technology collects data, what kind of data the technology collects, for what purpose the data is collected, and to whom and for what purpose the collected data is disclosed.
- Know which regulations apply to that data, whether consumer consent is needed, and what data collection, usages, or sharing must be disclosed in your privacy policy.

3) Know Your Regulations:

- Understand which laws and regulations apply to your entity, your activities, and any consumer health data collected on or through your digital interface or that your entity handles in any way. Many digital health tech companies are founded by former Sillicon Valley technology startup leaders who are unfamiliar with – and surprised by – the regulatory intricacies at play.

4) Integrate:

- Make sure your right arm is talking to your left arm, and that your insides match your outsides. In other words, your privacy policies, terms of use and vendor contracts need collaborative review by your IT and compliance departments, and coordinated with your vendors' data practices.

5) There's A Lot at Stake:

- Digital health companies and entities subject to HIPAA often neglect to consider the FTC, but from websites to mobile apps to wearables, the FTC isn't neglecting them. The FTC is taking a no-nonsense approach to holding companies responsible for data misuse and exposure. The Baker's Dozen's entertainingly edgy tone should not distract from its stern message, to think carefully about the way your own practices line up with the Baker's Dozen principles or risk significant penalties for your

company and maybe even yourself. Do your company (and yourself) a favor and check them out.

The author would like to thank Zoe Dettelbach for her contribution to this post.

[1] The Health Insurance Portability and Accountability Act.

[2] California Consumer Privacy Act.

[3] California Privacy Rights Act.

[4] While this post does not cover state law, the April 2023 Washington State's "My Health My Data Act" and, in particular, its inclusion in certain contexts of information inferred from nonhealth data, is a game changer.

[5] HHS OCR is the Department of Health & Human Services Office for Civil Rights. HHS OCR is the agency that enforces HIPAA.

[6] For more on covered entities and business associates under HIPAA, see https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[7] See Footnote 2.

If you have any questions or would like more information about these developing issues, please contact the following:

KATHERINE LEIBOWITZ
1-610-896-5788
Katherine.Leibowitz@LeibowitzLawTeam.com