RETROSPECTIVE

US POLICY

# FPF Health & Wellness:

## Mapping the 2024 Health Privacy Landscape

*A 2023 Retrospective*

Author: Jordan Wrigley, FPF, February/2024

FUTURE OF PRIVACY FORUM

## Table of Contents

## Introduction

In 2024, health and wellness-focused companies are increasingly integrating AI to streamline their services–with the expansion of AI-enabled digital health, the universe of potential health inferences will also expand, triggering new concerns about patient and consumer privacy. At this intersection of reproductive health privacy and AI concerns, state legislators and federal regulators appear poised to take more action on health data privacy, with specific attention to reproductive health privacy and genetic data privacy. As we look ahead to further developments, it is prudent to look back and understand exactly where the regulatory landscape stands and how we got here...

In 2023, health data privacy developments were nearly all related to the continuing development of privacy law responses to the Supreme Court's *Dobbs* decision and subsequent moves by states to bar access to certain reproductive health care services and to criminally prosecute individuals seeking access to that care. As reproductive health care remains in jeopardy in several states, we expect that reproductive health data privacy will continue to drive broader action on health data privacy. In this 2023 retrospective, we have identified top themes of health legislation and regulation.

***Theme One: Law enforcement access to data***

Beginning in 2022 and continuing throughout 2023, states and federal actors, as well as individual organizations, took steps to restrict law enforcement access to reproductive care data. For example, a group of states with legal protections for abortion, including California, New York, and Washington, passed laws restricting the ability of out-of-state law enforcement to request information from entities about reproductive care services lawfully obtained within the state.

Additionally, the U.S. Department of Health and Human Services's Office for Civil Rights (OCR), issued a Notice of Proposed Rulemaking notifying the public of its intention to pass a rule extending additional protections to reproductive health care data under the HIPAA Privacy Rule. The proposed rule would prohibit regulated entities from disclosing an individual's personal health information (PHI) to law enforcement for reproductive care-related investigations or prosecutions when such care was lawfully obtained. The Proposed Rule would also expand the Privacy Rule's definition of "health care" to include "reproductive health care," including prenatal care, abortion care, and use of contraceptives.

*IN 2024*: We will expect to see a final rule issued by HHS OCR, as well as further legislative efforts in various U.S. states to control the flow of health data (and reproductive health data specifically) across state and federal borders.

***Theme Two: Organizational collection, use, & disclosure of data***

In 2023, we saw the introduction and passage of a number of novel state-level health privacy bills that impact how organizations can collect, use, and disclose health data. The most prominent of these bills was Washington State's 'My Health, My Data' Act, which covers broad categories of health data and health-related inferences. There were also peer bills in Nevada, Connecticut, and New York, where legislators sought to place limits on private entities' collection, use, and disclosure of individual's non-HIPAA covered health information and/or to restrict the geofencing of health care facilities for the purpose of identifying, tracking, or sending messages to people entering those facilities.

Last year also marked a watershed moment for the Federal Trade Commission's (FTC) health privacy enforcement agenda. The FTC entered into settlement agreements with a number of companies, including Vitagene, GoodRx, BetterHelp, & Premom. In these actions, the FTC adopted a broad definition of sensitive health information; entities must obtain express consumer consent to collect, use, or share sensitive health information, which includes personal information (e.g., emails, IP addresses, etc.), if such information is connected to an individual's efforts to research or obtain health services.

*IN 2024*: Already, three states have introduced some version of legislation based on 'My Health, My Data'. Vermont (S. 173) and Hawaii (HB 1566) are MHMD 'look-alike' bills. Meanwhile, Illinois (HB 3080) contains significant yet nuanced definitional differences and does not explicitly include reproductive care, gender affirming, or biometric data.

***Theme Three: Lawmaker consideration of "sensitive" health information and health inferences***

This past year, lawmakers and regulators also grappled with how to establish protections for data, with a focus on location data, which can be used to infer sensitive information about an individual's visits to health care facilities. For instance, the FTC filed an amended complaint in its ongoing litigation against location data broker Kochava, alleging that Kochava's sale of precise geolocation data that can be easily associated with individuals and used to infer information about visits to sensitive locations is an unfair trade practice in violation of Section 5 of the FTC Act.

Last year the FTC also issued an NPRM, regarding the Health Breach Notification Rule (HBNR). 2023 also saw the first application of the HBNR in enforcement actions against GoodRx and Premom/Easy Health Care since its implementation in 2010. The NPRM aims to "clarifying the rule's applicability to health apps and other similar technologies" and included revising definitions

and clarifying “an unauthorized acquisition of identifiable health information that occurs as a result of a data security breach or an unauthorized disclosure.”

*IN 2024*: We expect to see the results of the HBNR NPRM this year. The FTC has also continued to build on this location data enforcement agenda in early 2024, as data brokers X-Mode Social and InMarket have recently reached settlements about their sales of sensitive location data associated with healthcare. Meanwhile, in Massachusetts, lawmakers introduced the Massachusetts “Location Shield Act,” (H. 357) which was immediately endorsed by the Massachusetts ACLU. The bill, which is still being considered by the Massachusetts legislature during its two-year legislative session, would place a flat-out ban on the sale of an individual's phone location data to third parties; advocates for the bill have cited the many types of sensitive information that can be inferred from such data.

For more information, read the FPF resources!

- A New Paradigm for Consumer Health Data Privacy in Washington State (April 27, 2023)
- Connecticut Shows You Can Have it All (June 9, 2023)
- (Health) Data is What (Health) Data Does in Nevada (June 22, 2023)

## Scholarly Research Landscape of 2023

The landscape of consumer health data privacy is rapidly evolving, driven by changing laws, consumer demands, and technological advancements. The scholarly research landscape has largely followed some of the key issues in health data privacy regulation and enforcement: processing sensitive health data, incorporating AI in healthcare operations, and establishing standards for data sharing and deidentification. Here we provide a few of the major areas that researchers focused on in 2023:

- FemTech apps continue to be a top area of interest, with researchers assessing data privacy and security practices of menopause support and menstrual cycle tracking apps, along with the impacts of law enforcement access to data for individuals seeking care;
- Privacy risks around emerging technologies have been on researchers’ agendas, resulting in examinations of neurodata, biometric data repurposed as diagnostic data, and data collected from metaverse wearable devices;
- As generative AI and large language models (LLMs) have gained popularity in healthcare, researchers have also considered how LLMs can be used to optimize health records and what data sharing principles should be implemented for AI-driven research;
- Researchers have studied technical methods for implementing strong data governance principles, including blockchain and federated learning implemented in telemedicine, and

have suggested that certain techniques, including data deidentification, may need to be paired with stronger privacy protections to effectively mitigate risks

## FPF Analysis of Federal Trade Commission (FTC) Cases in 2023

***Sent to FPF Health & Wellness Working Group members on March 22, 2023.***

The FTC has been active in health data privacy enforcement actions, which included *GoodRx*, *Easy Healthcare (Premom)*, *BetterHelp*, *and 1Health.io/Vitagene* in 2023. FPF has followed the FTC's enforcement actions, and the Health and Wellness team is tracking how the FTC's enforcement agenda has prioritized health data privacy protection and deceptive claims about privacy and Health Insurance Portability and Accountability Act (HIPAA) compliance, and this enforcement agenda may suggest additional rulemakings in 2023. The comparison table below, previously sent to FPF Health and Wellness members, addresses three of the four key FTC enforcement actions taken this year.

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| Date of enforcement action: Feb 1, 2023<br>• FTC Press Release<br>• Link to Complaint; Proposed Order; and Concurring Opinion | Date of enforcement action: Mar 2, 2023<br>• FTC Press Release<br>• Link to Complaint; Proposed Order; and Concurring Opinion | Date of enforcement action: May 17, 2023<br>• FTC Press Release<br>• Link to Complaint; Proposed Order |
| **About:** | | |
| "Consumer-focused digital healthcare platform"..."advertises, distributes, and sells health-related products and services directly to consumers, including purported prescription medication discount products." | Company that provides "an online counseling service" including "specialized versions of the Service for people of the Christian faith, members of the LGBTQ community, and teenagers." | Company that develops, advertises, and distributes a mobile app called the Premom Ovulation Tracker ("Premom") that allows users to input and track various types of personal and health information. |
| **What they offer:** | | |
| • Offers a platform through its website or mobile app<br>• Claims consumers can save money using GoodRx to | • Users are prompted to fill out a questionnaire and create an account to access mental health | • App users can log information about their periods and fertility and upload pictures of |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| purchase prescription medications<br>• Offers online primary care visits (telehealth services)<br>• Consumers can use the company's services to keep track of their health information, including details about their prescription drug history | services<br>• User are matched with one of +25,000 licensed therapists<br>• Therapists provide users with mental health therapy via video conferencing, text messaging, live chat, and audio calls | ovulation test strips that the app can analyze to predict the user's next ovulation cycle<br>• Permits users to import their health data from other devices or apps<br>• Premom app offers an ovulation tracker, period tracker, and pregnancy resources for those trying to conceive |
| **What did they do?** | | |
| • Configured a Facebook pixel on its sites to send Facebook customer info (listed below)<br>• By using Facebook's ad targeting platform, GoodRx designed campaigns that *targeted* customers with *advertising* based on their health information<br>• GoodRx was able to identify customers who had Facebook and Instagram accounts and then used their Personal Health Information (PHI) to target them with ads on that platform | • Company made multiple statements on its website promising not to sell or share information (listed below)--including that customers are seeking or are in therapy, and whether they have previously been in therapy<br>• BetterHelp shared this info with Facebook, Snapchat, Pinterest and Criteo to *target advertising* about the company's services | • Repeatedly and falsely promised users in privacy policies that:<br>○ They would not share health information with 3Ps without users' knowledge or consent;<br>○ The data collected and shared was non-identifiable data; and<br>○ The data was used only for their own analytics or advertising; and<br>○ They would notify and obtain users' consent before using its users' data |

| GoodRx | BetterHelp | Easy Healthcare |
| --- | --- | --- |
| | | for any other purposes<br>● Software development kits (SDKs) from 3Ps were incorporated into the Premom app, which transferred Custom App Events to 3Ps, thus contradicting EHC's privacy policies<br>● Google and AppsFlyer's SDKs disclosed health info to them thru "Custom App Events"<br>○ SDKs collected users' unique advertising or device identifiers (can be used to track consumers across the internet and apps, and used to match an actual person to their own lists – thus, associating reproductive health info to a specific individual)<br>○ Custom App Events titles were descriptive titles that conveyed health info about Premom users (ex: Calendar/Report/LogFertility) instead of anonymous names<br>● Umeng and Jiguang's (Chinese mobile apps) |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| | | SDKs integrated U-Share and JPUsh into Premom<br>○ U-Share - shared social media account info of users, sensitive data that identifies users<br>○ U-Share + JPush collected resettable, non-resettable identifiers, and precise geolocation<br>○ Sharing info with these 3Ps violated Apple and Google policies<br>○ EHC knew that these companies could use this data for their own business purposes or could transfer the data to other 3Ps and failed to disclose this info to Premom users |
| **PHI allegedly gathered:** | | |
| • First and last name<br>• Email address<br>• Phone number<br>• Street address<br>• IP address<br>• Date of birth<br>• Credit card info<br>• Prescription info<br>○ Name<br>○ Desired dosage | • Name<br>• Nickname<br>• Email address<br>• Phone number<br>• Emergency contact info<br>• Credit card<br>• IP address<br>• Age<br>• Sexuality<br>• Mental health info | • Dates of periods/menstrual cycles<br>• Progesterone and other hormone test results<br>• Moods<br>• Sexual history<br>• Sleep schedule<br>• Cervix mucus<br>• Body temperature<br>• Pregnancy and fertility |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| ○ Form<br>○ Quantity<br>• Health condition<br>• Medication purchase history<br>• Drug for which a user had received a coupon<br>• Health condition drug treated<br>• Users' latitude and longitude coordinates<br>• Unique advertising IDs | • Medications<br>• Sexual history<br>• Religion<br>• Therapy history | status<br>• Weight<br>• Pregnancy-related symptoms<br>• Precise Geolocation<br>• Resettable identifiers<br>○ Android ID<br>○ Android Advertising ID<br>• Non-resettable identifiers<br>○ HWID<br>○ IMEI<br>○ Router addresses<br>○ Bluetooth addresses<br>○ MAC addresses<br>○ SSIDs |
| **Violation of the Health Breach Notification Rule (HBNR)** | | |
| • The complaint charges that GoodRx is a "vendor of personal health records (PHR)" subject to the HBNR<br>○ GoodRx maintains "an electronic record of PHR identifiable health information on an individual that can be drawn from *multiple sources* and that is managed, shared, and controlled by or primarily for the individual."<br>○ GoodRx's website and Mobile Apps are electronic records of PHR | **FTC did not apply HBNR here**<br><br>From Wilson's concurrence:<br>• The info BetterHelp collected from consumers and provides to therapists on its platform *does not* constitute a PHR of identifiable health information under the HBNR because it does not include records that "can be drawn from multiple sources"<br>• A consumer provides their information to BetterHelp but the company *does not pull additional health information* from another source or vendor | • The complaint charges that Easy Healthcare (EHC) is a vendor of PHR subject to the HBNR because Premom "collects and receives PHR identifiable health information from multiple sources."<br>• EHC experienced "breaches of security" through disclosure and app events titles with 3Ps<br>• PHR identifiable health information was unsecured and shared with 3Ps without obtaining users' authorization<br>• PHR was not encrypted or rendered unusable when transferred to unauthorized 3Ps and was sent as |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| identifiable health information that are capable of *drawing information from multiple sources*, including inputs from users<br>• FTC stated GoodRx violated the HBNR by **failing to notify** the appropriate parties of a breach of unsecured PHR of identifiable health information<br>○ GoodRx should have notified customers, the FTC, and the media about the company's unauthorized disclosure of identifiable PHI to Facebook and Google<br>• A "breach" is not limited to cybersecurity intrusions or nefarious behavior<br>○ Incidents of unauthorized access, i.e., sharing covered information without an individual's authorization triggers notification obligations under the HBNR | | "Custom App Event titles in plain text"<br>• EHC's violation of the HBNR is "ongoing"<br>• EHC has not notified users that it breached the security of Premom users' PHR identifiable health info through unauthorized 3P disclosures |
| **Violation of Section 5 of the FTC Act** | | |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| ***Deception and Misrepresentation*** | | |
| **Privacy Misrepresentation:**<br>● Disclosure of Health Information to Third Parties (3Ps)<br>○ Represented it would not disclose PHI to advertisers or other 3Ps<br>○ Did disclose users' PHI to Advertising Platforms and other 3Ps (Facebook, Google, and Criteo)<br>○ Used the information to *target users* with health-related *advertisements* on Facebook and Instagram<br>● Disclosure of Personal Information to Third Parties<br>○ Represented it would use or disclose users' PI only for *limited purposes*, i.e., providing GoodRx's services to users or contacting users directly<br>○ Thru subsidiary HeyDoctor<br>■ Represented it would obtain users' consent before | **Privacy Misrepresentation**<br>● Disclosure of Health Information for Advertising and Third Parties' Own Uses<br>○ Represented it would not disclose consumers' health information to any 3P for *advertising* or that 3P's *own uses*<br>○ Disclosed consumers' health information to 3Ps (Facebook, Pinterest, Snapchat, and Criteo) for *advertising* and those 3Ps' *own uses*<br>● Use of Health Information for Advertising<br>○ BetterHelp represented it would not use consumers' health information for *advertising* or *advertising*-related purposes<br>○ Used consumers' health information for *advertising* and *advertising*-related purposes<br>● Disclosure of Health Information | **Privacy Misrepresentation**<br>● Disclosure of Health Information<br>○ Represented it would not disclose PHI to advertisers or other 3Ps<br>○ Did disclose users' PHI to other 3Ps (Google and AppsFlyer)<br>● Sharing Data with Third Parties<br>○ Represented to consumers they shared only non-identifiable (non-ID) information to 3Ps and that these 3Ps tracked users only by IP address<br>● Third Parties' Use of Shared Data<br>○ Represented it would not disclose users' info for any purpose other than those outlined in privacy policies and ToS<br>○ Represented that consumer data would be used and shared for EHC's own analytics and advertising<br>○ Representations |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| disclosing PI to 3Ps for *purposes beyond* providing users access to its services.<br>○ Disclosed users' personal information (PI) to Advertising Platforms for advertising<br>■ First and last name, physical address, email address, phone number, gender, and other personal identifiers<br>○ Used the information to identify and target users with health-related advertisements on Facebook and Instagram<br>● Failure to Limit Third-Party Use of Health Information<br>○ Represented it would take steps to limit 3P use of users' PHI by: | ○ Represented it would not disclose consumers' health information to anyone *except* each consumer's licensed therapist<br>○ Disclosed consumers' health information to at least one entity other than each consumer's licensed therapist (Facebook)<br>● HIPAA Certification<br>○ Represented that a government agency or other 3P had reviewed BetterHelp's privacy and information practices and determined that they met HIPAA's requirements<br>○ No government agency or other 3P had ever reviewed BetterHelp's privacy or information security practices and determined that they met HIPAA's requirements.<br><br>**Failure to Disclose**<br>● Disclosure of Health Information for Advertising | were false or misleading because EHC incorporated UShare and JPush into Premom, which conveyed users' PHI to Chinese 3Ps<br><br>**Deceptive Failure to Disclose**<br>● Sharing Geolocation Information with Third Parties<br>○ Represented to consumers that consumers needed to turn on location sharing so that Premom could locate consumers' Bluetooth thermometers<br>○ Failed to disclose they conveyed users' geolocation information to Chinese companies including 3P advertising which would be material to consumers in their decision to use EHC's services<br>● Third Parties' Use of Shared Data<br>○ Represented that consumer data would be used and shared for EHC's own analytics and advertising |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| ■ Ensuring that 3P complied with "federal standards" regarding the treatment of health information<br>■ Taking steps to ensure that 3P are subject to confidentiality obligations<br>○ Thru subsidiary HeyDoctor<br>■ Represented it would implement "contractual and technical protections" to limit 3P use of users' information, beyond use of information for the provision of telehealth services<br>○ Failed to take steps to limit 3P use of users' PHI | and Third Parties' Own Uses<br>○ Represented it would disclose consumers' health information to 3Ps for *limited* purposes<br>■ Listed purposes did not include advertising or 3P own uses.<br>○ Failed to disclose that it disclosed consumers' health information to 3Ps (Facebook, Pinterest, Snapchat, and Criteo) for advertising and 3Ps own uses<br>■ Would have been material to consumers in their decisions to use BetterHelp's services<br>● BetterHelp's Own Use of Health Information for Advertising<br>○ Represented it would use consumers' health information for limited purposes | ○ Failed to disclose that by incorporated UShare and JPush into Premom, which conveyed users' PHI to Chinese 3Ps, these companies could use and transfer user data for their own purposes<br>○ This info would be material to consumers in their decision to use EHC's services |

| GoodRx | BetterHelp | Easy Healthcare |
| --- | --- | --- |
| ■ 3Ps that received PHI (Facebook, Branch, Criteo, and Twilio) were permitted to make use of this information for their *own internal business purposes*, e.g., for their own research and development or ad optimization purposes.<br>○ Took insufficient action to limit what these 3Ps could do with users' PHI<br>■ Either agreed to each company's standard terms of service, or entered into agreements that permitted these 3Ps to use GoodRx | ■ Listed purposes did not include *advertising* or *advertising*-related purposes<br>○ Failed to disclose that it used consumers' health information for advertising and advertising-related purposes | |

| GoodRx | BetterHelp | Easy Healthcare |
| --- | --- | --- |
| users' PHI for their own internal business purposes.<br>• Misrepresenting Compliance with the Digital Advertising Alliance Principles<br>  ○ Represented that GoodRx adheres to the Digital Advertising Alliance's (DAA) principles, including its Sensitive Data Principle<br>  ○ Violated the DAA when it used PHI to target users with health-related advertisements on Facebook and Instagram, without obtaining users' affirmative express consent.<br>• HIPAA Compliance<br>  ○ Represented that GoodRx is a HIPAA-covered entity, and that its privacy and information practices were in compliance with HIPAA's requirements<br>  ○ GoodRx is not a HIPAA-covered | | |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| entity, and its privacy and information practices did not comply with HIPAA's requirements. | | |
| ***Unfairness*** | | |
| • Failure to Implement Measures to Prevent the Unauthorized Disclosure of Health Information<br>  ○ Failed to implement any sufficient policies or procedures to prevent the improper or unauthorized disclosure of users' PHI, or to notify users of breaches of that information<br>• Failure to Provide Notice and Obtain Consent Before Use and Disclosure of Health Information for Advertising<br>  ○ Collected and disclosed users' PHI to Advertising Platforms (Facebook) without users' knowledge, notice or consent<br>• Likely to cause substantial injury to consumers<br>  ○ Not outweighed by benefits | • Unfair Privacy Practices<br>  ○ Failed to employ reasonable measures to protect consumers' PHI in connection with the collection, use, and disclosure of that info<br>• Failure to Obtain Affirmative Express Consent Before Collecting, Using, and Disclosing Consumers' Health Information<br>  ○ Failed to obtain consumers' affirmative express consent before collecting, using, and disclosing to 3Ps those consumers' health information<br>• Likely to cause substantial injury to consumers that is not outweighed by countervailing benefits<br>  ○ Not outweighed by benefits | • Unfair Privacy and Data Security Practices<br>  ○ Failed to take reasonable measure to assess/address privacy and data security risks created by 3P software incorporated in Premom<br>  ○ Caused or likely to cause substantial injury to consumers that they cannot reasonably avoid and is not outweighed by countervailing benefits<br>• Unfair Sharing of Health Information for Advertising Purposes Without Affirmative Express Consent<br>  ○ Failed to encrypt or label Premom users' Custom App Events to prevent the transfer of users' PHR to |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| | | ○ Google and AppsFlyer<br>○ EHC transferred users' PHR to 3Ps without users' knowledge and without providing users notice or obtaining affirmative express consent.<br>○ Caused or likely to cause substantial injury to consumers that they cannot reasonably avoid and is not outweighed by countervailing benefits |
| **Terms of Proposed Order** | | |
| • Required to pay $1.5 million<br>• Prohibits deceptive practices outlined in complaint<br>• Required company to comply with HBNR<br>• Permanently prohibited from sharing user "health data" with applicable 3Ps for advertising purposes<br>• Required user consent for any other sharing of PHI with 3Ps for other purposes<br>• Required company to seek 3Ps deletion of data that was shared<br>• Limited retention of data<br>• Implemented mandated | • Required to pay $7.8 million - will be used to provide partial refunds to customers<br>• Prohibited sharing individually identifiable information relating to physical or mental health or condition(s) of a consumer with any 3P for advertising<br>• Prohibited sharing consumers' personal information more generally with 3Ps for the purpose of retargeting<br>• Limited future data-sharing<br>• Must contact affected consumers directly about | • Required to pay $100,000 to the U.S. Treasurer<br>• Permanently prohibited from disclosing health info to 3Ps for health purposes<br>• Permanently prohibited from misrepresenting about their health data collection, maintenance, disclosure or permission practices<br>• Permanently prohibited from disclosing health info to 3Ps for non-advertising purposes without affirmative express consent and notice<br>• Must provide proper notice if there is a breach of PHR |

| GoodRx | BetterHelp | Easy Healthcare |
|---|---|---|
| privacy program | the case and must direct 3P to delete consumers' health and other personal data that BetterHelp shared with them. | • Notify users of Order within 28 days<br>• Must identify all 3Ps that received health data from EHC and notify them of the FTC's allegations<br>• Must instruct all 3Ps (including Chinese companies) that received health data from EHC to delete this info<br>• Implement and maintain a privacy and information security program<br>• Must have its privacy and information security program assessed by 3Ps and properly cooperate with 3P assessor(s)<br>• Submit an annual certification to the FTC of compliance with Order<br>• Report to FTC of any future covered incidents<br>• Must submit a compliance report that:<br>  ○ Describes business activities (products and services offered)<br>  ○ Describes the means of advertising, marketing, and sales, and EHC involvement<br>• Must retain the following records:<br>  ○ Consumer complaints and |

| GoodRx | BetterHelp | Easy Healthcare |
| --- | --- | --- |
| | | refund requests related to any EHC offered mobile app or website, concerning the collection, use, maintenance, disclosure, deletion, or permission of access to covered info<br>○ All disclosures of PHR Identifiable Health Information to 3Ps – 3P name, address, disclosure date(s), purpose(s) for PHR transfer, how/when users provided authorization for disclosures<br>○ All disclosures of App Events to 3Ps<br>○ Each unique advertisement, form advertisement, other marketing material subject to this Order;<br>○ Each widely disseminated representation by EHC that describes that EHC maintains or protects the privacy, security, and confidentiality of any Covered Information |

## FPF Takeaways on GoodRx Settlement

***Original version sent to FPF Health & Wellness Working Group members on February 2, 2023.***

In February 2023, the FTC published a significant decision against GoodRx, a "consumer-focused digital healthcare platform." (Read the complaint and stipulated order). The decision represents a novel application of several areas of law to further the FTC's position that the collection, use, and sharing of sensitive health conditions by non-HIPAA entities requires affirmative consent. GoodRx has released a response on their website. Legal concerns arose primarily from a 2020 investigation from Consumer Reports exploring GoodRx's use of third-party advertising services, including the use of audience segments and profiles related to specific diagnoses.

A few initial observations from the FPF team:

- The complaint includes a number of novel legal issues, including a "first of its kind" application of the 2009 Health Breach Notification Rule (HBNR). Under the HBNR, the FTC found that GoodRx, as a (non-HIPAA) "vendor of personal health records" experienced "breaches of security" when it shared its users' identifiable health information with third-party advertising platforms without its users' knowledge or consent.

- In a significant ongoing trend, the FTC found that these same activities violated the "unfairness" prong of Section 5. The application of "unfairness" to the non-consented sharing and use of sensitive health information is consistent with the FTC's approach in Kochava (notably, the GoodRx complaint mentions, but does not address, GoodRx's collection and use of precise geolocation information).

- This is the first time (to our knowledge) that the FTC has expressly invoked non-compliance with the Digital Advertising Alliance (DAA) Principles as a basis for a deception claim. Similarly, the complaint alleges that the company's presentation of a HIPAA compliance certification on the webpage of their Hey Doctor subsidiary is deceptive for a non-HIPAA-covered entity. GoodRx has noted in a response that this "seal" was removed shortly after the acquisition of Hey Doctor in 2019.

- The complaint does not distinguish between sensitivities of different types of health-related information, including examples of ad campaigns related to conditions that could be perceived as low-sensitivity (e.g. Blood pressure or Lipitor), as well as health conditions that are considerably more sensitive (e.g. Zolpidem). The GoodRx response states that "[n]o medical records were shared."

- Notably, the decision follows a 2021 FTC notice advising consumer-facing "health apps and connected devices" that they must comply with the Health Breach Notification Rule. Although that notice was approved 3-2, this decision was 4-0. Commissioner Wilson's concurring statement notes that she would have supported higher penalties.

## FPF Takeaways on Premom (Easy Healthcare) Settlement

***Original version sent to FPF Health & Wellness Working Group members on May 22, 2023.***

The FTC published another case in a series of significant decisions around consumer health data and privacy in May 2023. The complaint is against Easy Healthcare, the creator and purveyor of the Premom app, an "ovulation prediction app" and other fertility tools. (Read the complaint and proposed order). The decision represents the second application of the Health Breach Notification Rule (HBNR) and continues a trend of scrutinizing the sharing of "user personal health data" with third parties for the purposes of advertising.

The settlement was announced on the same day as the FTC's monthly Open Meeting, in which the Commission voted 3-0 to begin formal rulemaking on the HBNR, and 3-0 to issue a Policy Statement on biometric data. The rulemaking goal is to clarify the scope of entities and technologies that are covered by the HBNR.

Takeaways on 'Easy Healthcare' from the FPF team:

- **The Agency's Action Comes After a Previous Investigation:** This complaint and order comes after an investigation by the International Digital Accountability Council (IDAC) which resulted in letters being sent to the Federal Trade Commission, Illinois Attorney General, and Google. IDAC is a digital watchdog organization incubated and launched from FPF in 2018.

- **Similarities to 'Flo Health; (2021):** The complaint contains several similarities to the 2021 complaint against Flo Health, a period and fertility-tracking app. Both Flo and Easy Healthcare were developers of fertility apps that violated their privacy promises and shared user data with third-parties. Both apps have period and ovulation tracking capabilities. The FTC viewed the data collected by both parties as sensitive health data that required responsible handling and should not have been exploited.

- **The Agency Remains Focused on "Reasonableness:":** The FTC is focused on consumer health data privacy in a way that is clearly new, but the agency hasn't abandoned its more vintage priorities. In a move that might be described as "classic FTC," the complaint

alleges Easy Healthcare and Premom “failed to implement ‘reasonable’ privacy and data security measures.”

- **Second Application of the HBNR:** After the recent GoodRx complaint, this is the second time the FTC has applied the Health Breach Notification Rule (HBNR) to the unauthorized disclosure/sharing of health information from a commercial app. The FTC found that Easy Healthcare, through the Premom app, was a (non-HIPAA) “vendor of personal health records" that experienced “breaches of security” when it shared its users’ identifiable health information with third-party advertising platforms and via third-party software development kits (SDKs).

- **Software Development Kits (SDKs):** The complaint alleges Easy Healthcare integrated two SDKs, U-Share and J-Push, into the Premom app without appropriate consideration or development of data use agreements allowing the uncontrolled collection and re-use of app users’ health data associated with personal identifiers.
    - One SDK “circumvented Android’s privacy controls and exploited a known bug in order to acquire Premom users’ Wi-fi MAC addresses.” The complaint also found the SDK’s privacy policies to be incongruent with the Premom app’s privacy policy.

- **Non-resettable identifiers:** Some identifiers (ex: device serial number or International Mobile Equipment Identity number) are “hardcoded” into hardware like a cellphone and may not be dissociated from collected data without the user purchasing a new phone. In ‘Easy Healthcare,’ the agency emphasizes the particular harm that comes from unauthorized disclosures of non-resettable identifiers, which will follow consumers in perpetuity unless they take drastic measures (like purchasing an entirely new mobile device). The difference between resettable and non-resettable identifiers has not been previously drawn out by the FTC, as noted in a report of the IDAC investigation.
    - The recent complaints against GoodRx and BetterHelp have illustrated that identifiers such as IP addresses and emails may be considered health information when drawn from a health context. Count VI of the complaint notes an increased risk of injury to users when non-resettable identifiers are implicated.

- **Custom Events:** Similar to previous cases, Easy Healthcare allegedly created unencrypted and unprotected Custom Events that were assigned names revealing of health information.n tandem with identifiers, this use of third-party analytics tools created an unauthorized disclosure of individually identifiable health information (IIPI).

## FPF Takeaways on Vitagene Settlement

***Original version sent to FPF Health & Wellness Working Group members on September 11, 2023.***

In September, the Federal Trade Commission ("FTC") finalized its order regarding the Commission's June 2023 settlement with 1Health.io, formerly known as Vitagene ("Vitagene"). The company develops and sells health-related products, including DNA test kits, to consumers. The FTC's Complaint and Consent Order are primarily focused on the company's DNA test-kit-related activities. The settlement is the fourth in a string of health privacy-based enforcement actions in 2023, and the first FTC settlement to focus on genetic privacy and security. The Commission voted 3-0 to issue the proposed administrative complaint and to accept the consent agreement with Vitagene.

The Complaint, in which the FTC alleged five counts under Section 5, asserts that Vitagene significantly over-promised and misrepresented its privacy and security programs while engaging in insufficiently protective data practices. Such practices allegedly included: failure to destroy DNA saliva samples after promising to do so; failure to sufficiently and effectively honor data deletion requests; implementing material, retroactive privacy policy changes; and failure to uniformly apply basic safeguards to the sensitive personal data stored on cloud services. It is worth noting that these practices would also violate the Future of Privacy Forum's (FPF) "Privacy Best Practices for Consumer Genetic Testing Services," a set of principles which have been agreed to and codified by the leading companies operating in the consumer genetic testing space.

The FTC's finalized order requires Vitagene to pay $75,000 toward consumer refunds, requires Vitagene to instruct third parties with whom physical DNA samples were shared to destroy those samples within 180 days, and prohibits the company from sharing health data with third parties without consumer consent.

**Takeaways on Vitagene from the FPF team:**

- **The Action is the FTC's First Genetics-Privacy Focused Complaint:**
    - The FTC has only brought a Section 5 complaint against a genetics company once before, in a 1991 case that did not involve privacy or security practices. Rather, it arose from allegedly "false and unsubstantiated claims regarding the success of [the company's] in vitro fertilization program."
- **The Evolution of "Health Information" Definitions Continues:**

- The order defines "Health Information" as "individually identifiable information relating to the *health or genetics* of an individual, including information: (1) concerning the propensity of that individual to develop a health condition; (2) concerning an analysis of the individual's DNA, RNA, chromosomes, proteins, or metabolites, in whole or in part; or (3) relating to the past, present, or future physical or mental health or conditions of an individual or the provision of health care to an individual" (emphasis added).
- Defining health information as information related to an individual's "health ***or*** genetics" creates a broad scope that would encompass the majority of information collected by genetics companies or products.

- **Material, Retroactive Privacy Policy Changes (Still) Aren't Okay:**
  - The complaint alleges that Vitagene acted unfairly by making significant retroactive changes to its privacy policy. Until April 2020, Vitagene's privacy policy stated that the company would only share individual's personal information, including health and genetic data, with third parties under "limited circumstances for narrow purposes," such as to provide customer-requested services. In 2020, without informing impacted individuals and with retroactive application to previously collected data, Vitagene changed its privacy policy to state that Vitagene could share customer data with third parties including "pharmacies, supermarket chains, nutrition and supplement manufacturers, and other providers and retailers" for a wide range of purposes, including for advertising.
  - The FTC has long held the view that, when companies make material, retroactive changes to their privacy policies, they must inform impacted individuals of these changes and obtain consumer consent to use previously-collected data in new ways. Here, Vitagene's privacy policy governed the company's sharing of genetic data, which, like biometric data, remains relatively static throughout an individual's lifetime in almost every case. This enduring quality of genetic data raises stakes, making Vitagene's retroactive changes particularly risky for individuals. In this case, the FTC's settlement agreement with Vitagene requires the company to obtain consumers' affirmative express consent before disclosing their health data to third parties.

- **Announced Privacy Policy Changes can be Unfair–Even When Unimplemented**
  - It is important to note that the FTC alleged that Vitagene's material, retroactive policy changes were unfair, *even despite* the fact that Vitagene never

implemented those changes. This suggests that there is risk for companies that announce forthcoming, objectionable changes to their privacy policies, even when they subsequently modify or abandon those changes in the face of regulator or customer objections. Indeed, the Vitagene Complaint appears to leave a door open for the possibility that the FTC might at some point bring a free-standing unfairness claim against a business for announced, but not enacted, privacy policy changes alone.

- **Inappropriately Partitioned Identifiers and Health Data are a Compliance Risk:**
    - Vitagene allegedly stored identifiable information (consumer's first names) in a way that could be or was linked with individuals' "Health Reports" or data derived from genetic testing and "other raw genotype data." Such data management practices may have contributed to the company's inability to fully delete consumers' data on request.
    - Storing identifiable information (e.g. names, IP addresses, etc.) and health data together with insufficient partitioning is a consistent theme in the FTC's 2023 health enforcement actions. Kate Black (Hintze Law) previously noted that combining identifiable information with health data *de facto* creates individually identifiable health information.
- **Why No Health Breach Notification Rule (HBNR) claims?**
    - The complaint alleges that Vitagene, despite repeated warnings from security researchers, stored raw consumer genetic data in a publicly accessible online database for several years, thus "expos[ing] online the health and genetic information of more than 2,600 consumers."
    - Despite this allegation, Vitagene ultimately informed the impacted consumers of this breach, which is why the Commission's complaint does not allege an HBNR violation. This is a good reminder that entities breach the HBNR when they *fail to notify* consumers about data breaches–not when that breach itself occurs.

## FPF Comments Submitted in 2023

FPF's Health and Wellness submitted two comments on proposed federal rulemaking about health data privacy protections:

1. a Notice of Proposed Rulemaking (NPRM) from the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to extend protections for reproductive health data covered under the Health Insurance Portability and Accountability Act (HIPAA).
2. the Federal Trade Commission's NPRM on expanding the scope of the Health Breach Notification Rule.

FPF also submitted comments in response to a Request for Information from Sen. Bill Cassidy (R-LA, Ranking Member of the Health, Education, Labor, and Pensions Committee). In all of these comments, which are included below, FPF's Health & Wellness team reiterated the importance of establishing clear definitions, providing detailed regulatory guidance, and protecting particularly sensitive categories of health data, including reproductive health data and genetic data.

In 2024, the FPF Health and Wellness team will continue to follow federal agencies' rulemaking processes around health data. The FTC, in particular, has been active on health data privacy enforcement actions. FTC Bureau of Consumer Protection Director Sam Levine has highlighted that the agency's rulemaking agenda focuses on its enforcement actions, which have collectively prohibited the practice of sharing sensitive health data in advertising. As the FTC continues to be more active in health data enforcement actions and HHS continues to address protections for reproductive health data post-*Dobbs,* FPF expects additional rulemaking in 2024 and will continue to put forth privacy recommendations for federal agencies' consideration.

## FPF Files Comments with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights

***Original summary published June 29, 2023***
***Comments filed June 15, 2023***

On June 15, the Future of Privacy Forum (FPF) filed comments with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) regarding the Notice of Proposed Rulemaking (NPRM) on extending additional protections to reproductive health care data under the Health Insurance Portability and Accountability Act (HIPAA).

In June 2022, the Supreme Court issued a decision that has resulted in loss of access to reproductive care for many Americans. Federal and state legislative and regulatory entities were quick to respond to protect rights to reproductive care, a fundamental aspect of decisional privacy. Rulemakings such as this one by HHS OCR sought to fill the gap left in the wake of the Supreme Court's 2022 decision that fundamentally shifted the landscape of data and information privacy. With a post-Dobbs lens, FPF filed comments on this rulemaking based on the following recommendations.

We recommend that HHS bolster privacy safeguards and support the responsible handling of reproductive health care information (RHCI) by specifically:

- Ensuring that covered entities are aware of and responsible for information that, directly or indirectly, can reveal data about individuals seeking or receiving reproductive health care;
- Providing additional guidance and resources to address the information privacy responsibilities of covered entities for their business associates and vendors;
- Distributing privacy education and guidance materials to covered entities and partners on data privacy transparency;
- Conducting regulatory analysis and providing compliance support for small clinics and rural/remote providers facing increased legal requests for reproductive and related health information;
- Addressing privacy protections for reproductive health care data collected and generated during and as a part of clinical research.

FPF's full comments to the HHS are available here.

## FPF Files Comments for the FTC Health Breach Notification Rule Addressing Specific Definitions and Clarity of Scope

***Original summary published August 10, 2023***
***Comments filed August 8, 2023***

On August 8th 2023, the Future of Privacy Forum (FPF) filed comments with the U.S. Federal Trade Commission (the Commission) regarding the Notice of Proposed Rulemaking (NPRM) to clarify the scope and application of the Health Breach Notification Rule (HBNR).

The HBNR was promulgated in 2009 as part of the American Recovery and Reinvestment Act as a breach of security rule. Recent complaints brought by the Commission, GoodRx and Easy Healthcare, were the inaugural and second application of the HBNR and indicated a novel range of alleged privacy breaches rather than traditional security breaches. The cases indicated a shift in the interpretation of "breach of security" by the Commission that drew many proto-typical practices into scope. The NPRM seeks to clarify this broadened scope which has amalgamated traditional breaches of security with nascent breaches of privacy. To draw out and address key issues in the NPRM and the Commission's considerations, we recommended that the

Commission consider the nuance of definitions and address the complexities of breach by specifically:

- Define a Standard for Identifiability for "PHR identifiable health data" to Clearly Expand Protections for a Broad Spectrum of Personal Information
- Define "Relates to" to Include the Creation of Health-Related Inferences from a Wide Range of Routine Commercial Datasets, While Establishing Clear Obligations for Businesses
- Establish Clear Guidelines for Intentional Data Sharing that Does Not Require Affirmative Consent
- Ensure that the Rule Contains "Good Faith" Exceptions for Merely Technical Violations
- Further Define "Breach of Security" to Clarify Where the Commission May Take Enforcement Action

FPF's full comments to the Commission are available here.

## Comments Submitted to Sen. Bill Cassidy (R-LA, Ranking Member of the Health, Education, Labor, and Pensions Committee) Regarding a Request for Information

***Comments sent September 26, 2023 via Electronic Mail***

Bill Cassidy, M.D., Ranking Member
U.S. Senate Committee on Health, Education, Labor, and Pensions
Washington, D.C. 20510-6300

Re: Feedback on health data privacy questions

Dear Ranking Member Cassidy,

On behalf of the Future of Privacy Forum (FPF), we are pleased to provide feedback on your office's request for information (RFI) on improving Americans' health data privacy.[1] We recommend that your efforts on health privacy reflect individuals' evolving, practical understandings of personal data and its use as well as the robust legislative and regulatory landscape. FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United

[1] Ranking Member Cassidy Seeks Information from Stakeholders on Improving Americans' Health Data Privacy, U.S. Senate Committee on Health, Education, Labor, & Pensions (September 7, 2023).

States and globally.[2] We seek to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective rules.

**Key considerations highlighted by our comments include**:

1. Definitions of "health data" in the non-Health Insurance Portability and Accountability Act (HIPAA) context are evolving and may be most effective when focused on processing purpose;
2. It is critically important for consumers to understand whether they are within or outside of a HIPAA-covered interaction when consenting to collection and use of their data;
3. Genetic data, which is particularly sensitive, should be protected by a robust privacy and security framework.

If you would like additional information or have questions on any of the information provided herein, you may contact Felicity Slater, Policy Fellow, at fslater@fpf.org.

Sincerely,
Felicity Slater, Policy Fellow
Jordan Wrigley, Researcher for Health & Wellness

**General Privacy Questions**

***Question 1*: What is health data? Is health data only data governed by HIPAA, or are there other types of health data not governed by HIPAA? Should different types of health data be treated differently? If so, which? How? If not, why not?**

We address this question in three parts. First, we discuss how health data is defined in the HIPAA context. Second, we discuss some considerations for how health data should be defined for privacy law purposes outside of HIPAA-contexts. Finally, we provide a comparative overview of current definitions of "sensitive data" and "health data" in state privacy laws and in recent Federal Trade Commission (FTC) Settlement Orders, and discuss these definitions.

*A. Health Data in the HIPAA Context*

The Health Information Portability and Accountability Act (HIPAA) is primarily an information portability law, intended to facilitate the transfer of health records.[3] While HIPAA was not drafted to be an information privacy law, the HIPAA Privacy Rule, which applies to HIPAA covered entities

[2] The views expressed in this comment are those of FPF and do not necessarily represent the opinions of our supporters or Advisory Board.
[3] Health Insurance Portability and Accountability Act of 1996 [hereinafter HIPAA], codified at 110 Stat. 1936.

and their business associates and was promulgated by the U.S. Department of Health and Human Services (HHS), creates important protections for certain individually-identifying protected health information (PHI).[4] The HIPAA Privacy Rule defines "individually identifiable health information" as:

> "information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."[5]

As this definition reveals, the HIPAA Privacy Rule does not cover data that is not individually-identifying (or potentially individually-identifying), nor does it cover data that is collected, stored, or transferred by a non-HIPAA covered entity, such as a consumer-facing health app, prescription service, or fitness tracker.[6]

### *B. Non-HIPAA covered Health Data*

When considering how "health data" should be defined outside of HIPAA, it is important to recognize the full context around the complex U.S. legislative and regulatory health data landscape. Any newly developed health privacy frameworks should account for leading global and U.S. privacy standards, in particular a definition of "personal information" that incorporates standards of reasonable identifiability that do not rest on an organization's beliefs or knowledge.[7] In the health data privacy context, this would mean developing privacy frameworks that protect health information when it is "linked or reasonably linkable to an identified or identifiable

---

[4] The HIPAA Privacy Rule, The U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,care%20providers%20that%20conduct%20certain (last visited: 9/21/23).

[5] The HIPAA Privacy Rule § 160.103.

[6] Tawanna Lee & Antonio Reynolds, "All Data Is Not HIPAA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulating the Health IoT Ecosystem," JD Supra (Jul. 13, 2021) ("most wearable devices, healthcare applications, and health IoT devices do not involve receipt, review, collection, or maintenance of health data by a Covered Entity. Instead, these consumer-driven products involve collection and storage of consumer-inputted data by device manufacturers and developers, who are not themselves Covered Entities. Without the Covered Entity nexus, this data remains unprotected.")

[7] Jordan Wrigley, Tatiana Rice, Felicity Slater, & Stephanie Wong, 'FPF Files Comments For The FTC Health Breach Notification Rule Addressing Specific Definitions And Clarity Of Scope,' (Aug. 10, 2023), https://fpf.org/blog/fpf-files-comments-for-the-ftc-health-breach-notification-rule-addressing-specific-definitions-and-clarity-of-scope/.

individual."[8] In addition, definitions of "health data" in privacy frameworks should account for the fact that information that may not be facially "health data" can nonetheless be queried to generate identifiable health data. A clear example of this occurs when an individual's location data is used to infer information about their health, based on their visits to certain locations–such as a pharmacy or treatment facility– and information about those visits, such as their duration or frequency.[9]

We have attached a 'Definitions of Health Data' Chart (see *Attachment 1)*, which provides an overview of how "health data" is treated under state comprehensive and health-specific privacy laws, as well as in recent Federal Trade Commission (FTC) Settlement Orders. State lawmakers are responding to concerns about health data privacy by drafting new legislation that seeks to protect consumer health data in two main ways. First, in each of the twelve generally-applicable state comprehensive privacy laws enacted thus far, health data is included within the definition of "sensitive data," and is subject to enhanced protections. Second, legislators in several states have introduced general consumer health data privacy laws, which seek to regulate how covered entities collect, use, and share non-HIPAA covered consumer health data.

*i. State Comprehensive Privacy Laws*

State comprehensive privacy laws generally include consumer health data within their definition of "sensitive data," and typically prohibit covered businesses from collecting or processing sensitive data without consumer consent.[10] California's comprehensive privacy law, which does not require individual consent for the processing of sensitive data, establishes that people have the right to, "at any time...direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average

[8] Id.
[9] *See, ex.* Patience Haggin, "Phones Know Who Went to an Abortion Clinic. Whom Will They Tell?," The Wall Street Journal (Aug. 7, 2022), https://www.wsj.com/articles/phones-know-who-went-to-an-abortion-clinic-whom-will-they-tell-11659873781.
[10] *See Attachment 1; see, ex.,* The Colorado Privacy Act (CPA) at Colo. Rev. Stat. § 6-1-1308(7) ("A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent, or, in the case of processing of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian;" Connecticut Data Privacy Act (CDPA), Public Act No. 22-15 at § 6.(a)(4) ("A controller shall...not process sensitive data concerning a consumer without obtaining the consumer's consent).

consumer who requests those goods or services."[11] In these laws, health data is usually covered by a variation of the phrase "personal information revealing of health diagnosis or condition."[12]

This definition of sensitive data raises several questions that many states have yet to resolve, including the scope of what constitutes a "health…condition" and if this scope is broader or narrower than "health diagnosis," or other, similar terms. It is also unclear what it means under the law for personal information to be "revealing of" health information. Courts, enforcers, and regulated entities will have to grapple with these questions as state comprehensive privacy laws continue to come into effect.

At least one state, Colorado, in its implementing regulations for the Colorado Privacy Act (CPA), has contended with this second question.[13] Colorado's rules define "[p]ersonal data revealing of…a mental or physical health condition or diagnosis" as including "sensitive data inferences." The text of the rule notes that, "precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual's health condition or sex life is considered Sensitive Data."[14] Thus, although Colorado is the only state that does not treat precise geolocation information as sensitive by default under its comprehensive privacy law, it does recognize that such information is sensitive when *processed* in order to reveal health information about a consumer. This expansion reveals an emerging trend in state privacy laws: treating certain categories of precise geolocation information, when processed in order to reveal information about an individual's health care choices, as sensitive data subject to enhanced protections.

*ii. Consumer Health Privacy Bills*

In addition to comprehensive privacy legislation, in 2023 many states have passed a second set of bills, which specifically regulate the collection, use, and transfer of consumer health data, defined broadly. The two most prominent legislation in this category are Washington State's 'My Health, My Data' (MHMD) Act and Nevada's Senate Bill 370 (SB 370) (see *Attachment 1)*, MHMD regulates collection and transfers of "consumer health data," defined as any form of "personal

[11] The California Consumer Privacy Act (CCPA), as modified by the California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.121.
[12] *See, ex.* The CPA at § 6-1-1303(24)(a) ("[s]ensitive Data…means…Personal data revealing…a mental or physical health condition or diagnosis"); The Virginia Consumer Data Protection Act (VCDPA), at Va. Code. Ann. § 59.1-571. ("[s]ensitive data…means a category of personal data that includes: ….mental or physical health diagnosis.").
[13] The Colorado Privacy Act Rules, 4 Colorado Code of Regulations 904-3, available at: https://www.coloradosos.gov/CCR/eDocketDetails.do?trackingNum=2022-00603.
[14] Id.

information" that "identifies the consumer's past, present, or future physical or mental health status." MHMD also provides a non-exhaustive list of 13 categories of information that constitute de facto "health status" under the Act, including "[p]recise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies," and health information that is inferred from non-health data. This MHMD definition of health data is significantly broader than the definitions established by other contemporary legal frameworks, including state comprehensive privacy laws, and will encompass information that has not historically been treated as health data.

By contrast, Nevada SB 370 applies to a narrower, use-based range of "consumer health data," specifically, information that a regulated entity "*uses* to identify the past, present or future health status of the consumer" (emphasis added). Furthermore, SB 370 excludes certain personal information concerning a person's shopping habits and interests. This narrower SB 370 definition excludes personal data that is not processed for health purposes and likely excludes certain information that industry representatives expressed concern could be captured under MHMD, such as purchasing ginger from a grocery store or subscribing to a fitness influencer. As such, SB 370's definition of "health data," although it is narrower than MHMD's, appears to effectively address the sort of data collection and processing that implicates health privacy concerns, including inferences of information about individual's health derived from information that is not, on its face, health-related.

**Collection of Health Data**

***Question 2:*** **How should information about data collection practices be conveyed to patients (i.e. plain language notice prior to consent, etc.)?**

For individuals, particularly when they operate in digital health spaces outside of the clear bounds of a physical healthcare building, it is crucially important to understand whether any given interaction with an entity is covered by HIPAA or not. The HIPAA Privacy Rule does not contain a mandatory consent requirement because HHS determined that such a requirement "would have posed barriers to health care."[15] Conversely, in the consumer space, consent often serves as the basis for data collection, transfer, and use, despite the fact that commenters have long discussed

[15] *See* "Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?," The U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/193/why-was-the-hipaa-privacy-rule-consent-requirement-removed/index.html (last visited: Sept. 22, 2023).

the limits of the notice-and-consent model as a privacy preserving measure in digital spaces.[16] Recent collaborative HHS and FTC products have noted the need for greater oversight of non-HIPAA entities that most closely mimic otherwise HIPAA-covered practices (ex. diagnosing, intervention selection and recommendation, detailed disease monitoring) or those entities who collect data that is analogous to information that would be collected by a provider or clinic.[17]

Individuals need tools to understand when they're relating to an entity as a *patient* (and thus providing information within the context of a HIPAA-covered exchange) or as a *consumer* (and thus providing information within the context of a non-HIPAA covered exchange). This may be particularly confusing for individuals when they move from a HIPAA-covered exchange into one that is not covered by HIPAA, such as from a digital interaction with a healthcare provider into a consumer pharmacy interface. Two recent FTC enforcement actions (GoodRx and BetterHelp) involved digital health spaces that combined HIPAA and non-HIPAA covered data collection where individuals spoke to providers (under HIPAA) and then provided information (outside HIPAA) to receive related services or provide data to improve products or support advertising.[18] Where such mixed regulatory spaces exist, there should be a bright line warning to individuals when their data that is being collected is protected under HIPAA and when it is not.

Within the HIPAA context, the HIPAA Privacy Rule puts forth several standards for communicating data collection and privacy rights. All patients and plan members must be given a Notice of Privacy Practices (NPPs) on the first encounter or as soon as reasonable. The NPPs must explain what PHI may be disclosed, to whom, and why, and must also explain an individual's right to access, amend, or transfer their PHI. If organizations violate the HIPAA Rules, individuals have the right to complain to either the organization or the HHS Office for Civil Rights (OCR).

---

[16] *See, e.g.,* Claire Park, "How "Notice and Consent" Fails to Protect Our Privacy," New America (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/; Cameron F. Kerry, "Why protecting privacy is a losing game today—and how to change the game," Brookings (Jul. 12, 2018), https://www.brookings.edu/articles/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/; Jedidiah Bacy, "Rethinking notice and consent — A chat with Jen King," The International Association of Privacy Professionals (Jun. 25, 2021), https://iapp.org/news/a/rethinking-notice-and-consent-a-chat-with-jen-king/.

[17] Lesley Fair, "Updated FTC-HHS publication outlines privacy and security laws and rules that impact consumer health data," The Federal Trade Commission (Sept. 15, 2023), https://www.ftc.gov/business-guidance/blog/2023/09/updated-ftc-hhs-publication-outlines-privacy-security-laws-rules-impact-consumer-health-data?utm_source=govdelivery.

[18] FTC v. GoodRx Holdings, Inc., No. 2023090 (N.D. Cal. Feb. 1, 2023); In re BetterHelp, Inc., No. 2023169 (Mar. 2, 2023).

The NPP model is also flexible and allows for communication of privacy practices and data collection in a range of formats to be inclusive of telehealth and other forms of healthcare provider interaction. The Privacy Rule also requires NPPs to use "plain language" and covered entities are "encouraged to develop notices that maximize readability and clarity."[19] Consent is not required and is voluntary rather than mandatory in order to facilitate the flow of information and remove barriers to care access.[20] Business associates are not required to adhere to the same NPP standards as providers. Covered entities who engage with a business associate must ensure contractual obligations regarding data collection and privacy by the business associate are in alignment with the covered entities' NPPs.

Genetic Information

***Question 1:*** **How should genetic information collected by commercial services be safeguarded?**

In July 2018, the Future of Privacy Forum released its *Privacy Best Practices for Consumer Genetic Testing Services* ("Best Practices").[21] This industry-leading self-regulatory framework was the result of a multi-stakeholder process that engaged technical experts, leading consumer genetic and personal genomic testing companies, and civil society, with input from regulators, including the Federal Trade Commission and the Department of Health and Human Services. Not only have FPF's Best Practices been broadly adopted by industry, but the Framework has formed the basis for genetic testing privacy laws in at least six states.[22] These laws recognize the sensitivity of genetic data by providing protections that go further than many existing sectoral privacy laws and laws of general applicability, and could serve as a helpful model for federal efforts to genetic data.[23] The Best Practices include strong standards for the use and sharing of genetic information generated in the consumer context including transparency, strict consent

[19] *See* "Summary of the HIPAA Privacy Rule," U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited: Sept. 21, 2023).
[20] *See* "Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?," U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/193/why-was-the-hipaa-privacy-rule-consent-requirement-removed/index.html (last visited: Sept. 21, 2023).
[21] Future of Privacy Forum, "Privacy Best Practices for Consumer Genetic Testing Services" (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[22] California (SB 41), Arizona (HB 2069); Utah (SB 277); Kentucky (HB 502); and Maryland (HB 866), and Virginia (SB 1087).
[23] California (SB 41), Arizona (HB 2069); Utah (SB 277); Kentucky (HB 502); and Maryland (HB 866), and Virginia (SB 1087).

requirements, consumer rights, limitations on use and onward transfer, and adherence to cybersecurity standards.

For instance, FPF's best practices include the recommendation that companies that store consumer genetic data maintain a comprehensive data security program. This program should be reasonably designed to protect the security, privacy, confidentiality, and integrity of genetic data against risks–such as unauthorized access or use, or unintended or inappropriate disclosure or breach–through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information. Genetic data should be protected through a combination of mechanisms including, at a minimum: secure storage of human biological materials and data, encryption of digital records, data-use agreements, and contractual obligations, and accountability measures (e.g. training, access controls and logs, and independent audits).[24]

***Question 2:*** **To what extent should information collected via commercial services be considered human subject research governed by the Common Rule?**

While the Common Rule applies to Federally-funded research and has not historically applied to research activities by commercial entities, there are examples of companies that voluntarily adhere to Common Rule provisions.[25] Mandating that the Common Rule apply to all companies' internal research, however, could pose significant practical challenges, such as creating new obligations for oversight capacity for the increased number of research protocol reviews. Despite these practical challenges, there is still a need to protect the interests, including the privacy interests, for individuals implicated by research that falls outside Common Rule scope. State comprehensive privacy laws provide some guidance as to how this may be accomplished.

Many state-level comprehensive privacy laws have exceptions for research that identify what steps researchers, including companies not legally bound by the Common Rule, must take to conduct research that is compliant and ethical.[26] Four of the most common provisions that guide research in these laws are below:

---

[24] Id.
[25] Federal Policy for the Protection of Human Subjects ('Common Rule'), The U.S. Department of Health & Human Services, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html (last visited: Sept. 22, 2023); Is All Human Research Regulated?, The U.S. Department of Health & Human Services, https://www.hhs.gov/ohrp/education-and-outreach/about-research-participation/protecting-research-volunteers/other-research/index.html (last visited: Sept. 25, 2023).
[26] *See ex.,* The CPA at §6-1-1304(2)(d); TheConnecticut Data Privacy Act (CDPA), Public Act No. 22-15 §10; The Virginia Consumer Data Protection Act (VCDPA), Va. Code. Ann. § 59.1-576(C)(4).

1. Researchers may "engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification."
2. Research "must be pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use."
3. "Complies with the Code of Federal Regulations (CFR) 21 Part 50." This regulation defines many of the protections for human subjects in research, defines informed consent, and describes additional protections for children in research.
4. "Complies with the Code of Federal Regulations (CFR) 21 Part 56." This regulation outlines when researchers are required to use an Institutional Review Board and describes their core functions and operations.

Institutional Review Board (IRB) review, or an equivalent process, can be another tool to ensure that privacy interests are respected even by non-Common Rule covered research. While IRBs predominantly operate within universities and are only available to people conducting certain types of research and affiliated with the university or who are in research partnerships with university affiliates, there are independent IRBs that companies can submit to when conducting research to meet the above provisions.

In Conclusion

FPF appreciates Ranking Member Cassidy's efforts to reflect on the privacy protections currently afforded to sensitive and identifying health information, both within and outside of the Health Insurance Portability and Accountability Act (HIPAA) context, and how those protections might be strengthened. Please reach out with any questions, and we look forward to speaking further about these important issues.

**Definitions of 'Health Data'**

| Category: State Comprehensive Privacy Laws | | | |
|---|---|---|---|
| **Law** | **Status** | **Scope** | **Relevant Definitions** |
| California Consumer Privacy Act, as modified by the California Privacy Rights Act (CPRA)<br><br>Cal. Civ. Code § 1798.199.10 et seq. | Enacted December 6, 2020, came into effect Jan. 1, 2023.<br><br>Modified Proposed California Consumer Privacy Act (CCPA) Regulations proposed October 17, 2022. | Covers businesses that collect and dictate the processing of consumer's personal information, do business in CA, and either: (1) had an annual gross revenue of over $25 million in the preceding calendar year; (2) buy, sell, or share the personal information of 100,000 consumers annually, or (3) gets 50% plus of its revenue from selling or sharing consumer personal information; as well as entities that control or are controlled by businesses that meet these requirements. § 1798.140 (d)(1)-(4). | "Sensitive personal information" means:...(2)(B) Personal information collected and analyzed concerning a consumer's health. *1798.140 (ae).* |
| Colorado Privacy Act (CPA)<br><br>Colo. Rev. Stat. § 6-1-1301 et seq. | Enacted July 7, 2021, came into effect July 1, 2023. | Applies to "controllers" that do business or target products and services at Colorado residents and either: (1) control or process the data of 100,000+ consumers per calendar year or (2) make money or receive a discount on goods or services from the sale of personal data and processes or controls the personal data of 25,000+ consumers. § 6-1-1304(1). | "Sensitive Data" means: Personal data revealing...a mental or physical health condition or diagnosis...*6-1-1303(24)(a).* |
| Connecticut Data Privacy Act (CDPA)<br><br>Public Act No. 22-15 | Enacted June 17, 2022, came into effect July 1, 2023. | Applies to businesses that do businesses in Connecticut or that make products and services targeted at Connecticut residents and that, in the prior calendar year: (1) controlled or processed the data of 100,000+ consumers or (2) controlled or processed the personal data of 25,000+ consumers and made more than 25% of their gross revenue from selling | "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis...*Section 1(27).* |

| | | | |
|---|---|---|---|
| | | personal data. §2. | |
| Virginia Consumer Data Protection Act (VCDPA)<br><br>Va. Code. Ann. § 59.1-571-§ 59.1-584 | Enacted March 2, 2021, came into effect January 1, 2023. | Obligations are imposed on entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that either:<br>- Control or process the personal data of at least 100,000 consumers during a calendar year, or<br>- Control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data. | "Sensitive data" means a category of personal data that includes: 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status...*§59.1-571.* |
| Utah Consumer Privacy Act (UCPA)<br><br>S.B. 277 Consumer Privacy Act | Enacted on March 24, 2022, will go into effect on December 31, 2023. | The UCPA applies to any entity that (1) conducts business in Utah, or produces products or services that are targeted to Utah residents; (2) has annual revenue of $25 million or more; and (3) annually controls or processes the personal data of at least 100,000 Utah residents, or controls or processes the personal data of at least 25,000 Utah residents and derives over 50% of its gross revenue from the sale of personal data. | "Sensitive data" means:...personal data that reveals:...information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional. *(32)(a)(i)(E)* |
| **Category: State Health-Specific Privacy Laws** | | | |
| **Law** | **Status** | **Scope** | **Relevant Definitions** |

| | | | |
|---|---|---|---|
| Washington 'My Health, My Data' Act (MHMD)<br><br>H.B. 1155 | Enacted April 27, 2023, substantive data privacy provisions will go into effect March 31, 2024 (or June 30, 2024 for small businesses), geofencing and enforcement sections came into effect July 23, 2023. | MHMD imposes obligations on "regulated entities" that "conduct[] business in Washington" and "produce products or services that are targeted to consumers in Washington" *§3(23)*, with blanket exemptions for three categories of organizations: government agencies, tribal nations, and "contracted service providers when processing consumer health data on behalf of a government agency" *§3(23)*).<br><br>MHMD creates a sub-category of regulated entities called "small businesses" that either: (a) "collect[], process[], sell[] or share[] the consumer health data of fewer than 100,000 consumers during a calendar year" or (b) derive less than 50% of their gross revenue from "the collection, processing, selling or sharing," of consumer health data and control the consumer health data of fewer than 25,000 consumers *§3(28)*. Small businesses are fully subject to MHMD.<br><br>Processors that "process consumer health data on behalf of a regulated entity or small business." *§3(23)* | "Consumer health data" is "personally identifiable information that is linked or reasonably capable of being linked to a consumer" and "identifies the consumer's past, present, or future physical or mental health status." *§3(8)(a)* This definition excludes personal information used public-interest research that is "approved, monitored, and governed by an institutional review board;" *§3(8)(c)*; information used for "public health purposes and activities" only; HIPAA-covered data; GLBA, FCRA, and FERPA-covered personal information; and information originating from a HIPAA-covered entity or business associate. *§12*<br><br>The act provides an inclusive list of examples of types of data that constitute "physical or mental health status," including:<br>"[H]ealth conditions, treatment, diseases, or diagnosis;<br>Social, psychological, behavioral, and medical interventions;<br>Health-related surgeries or procedures;<br>Use or purchase of prescribed medication;<br>Bodily functions, vital signs, symptoms, or measurements of information...;<br>Diagnoses or diagnostic testing, treatment, or medication;<br>Gender-affirming care information;<br>Reproductive or sexual health information;<br>Biometric data and Genetic data;<br>Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;<br>Data that identifies a consumer seeking health care services; or"<br>Health information that is derived or inferred from non-health data. *§3(8)(a)* |

| | | | |
|---|---|---|---|
| Nevada S.B. 370 | Enacted June 15, 2024, will take effect March 31, 2024. | Regulated Entities that "conduct business" in Nevada or "produce[] or provide[]" products or services targeted to Nevada consumers and solely or with others "determine the purpose and means of processing, sharing, or selling consumer health data." §15 Excluded from this definition are HIPAA & GLBA-covered entities; law enforcement agencies and activities; and the contractors of law enforcement agencies. *§20(1)(a)-(b) & (m)*<br><br>Processors that "process consumer health data on behalf of a regulated entity." *§14* | "Consumer health data" is "personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity uses to identify the past, present or future health status of the consumer." (emphasis added) §8<br>Excludes information used for certain research purposes; information used for public health purposes; FCRA and FERPA-covered personally-identifiable data; health data collected and shared as authorized by other state or federal law §20; information used to "provide access to or enable [video] gameplay;" and information used to "[i]dentify the shopping habits or interests of a consumer," if not used to infer health information. *§8(2)*<br><br>The act provides an inclusive list of examples of "consumer health data," including "information relating to:"<br>"[H]ealth condition or status, disease or diagnosis;<br>Social, psychological, behavioral or medical interventions;<br>Surgeries or other health-related procedures;<br>The use or acquisition of medication;<br>Bodily functions, vital signs or symptoms;<br>Reproductive or sexual health and Gender-affirming care;"<br>Health-related Biometric data or genetic data;<br>Precise geolocation information "that a regulated entity uses to indicate an attempt by a consumer to receive health care services or products; and"<br>Health information that is derived or inferred from non-health data. *§8(1)* |

| Category: Federal Trade Commission (FTC) Settlements | | | |
|---|---|---|---|
| **Case** | **Status** | **Case Description** | **Relevant Definitions** |
| GoodRx Holdings, Inc., FTC Docket No. 23-cv-460 (Feb. 1, 2023) | Finalized order issued February 17, 2023. | Digital health platform GoodRx deceived users by promising not to share personal health information with third parties. The company shared personal health information (prescriptions, health conditions, etc.) with third parties like Facebook, which then used the information to create targeted health-related advertisements. The FTC's complaint noted that GoodRx's deceptive privacy promises violated the FTC Act and that the unauthorized data sharing with third-party advertisers violated the Health Breach Notification Rule. GoodRx was fined $1.5 million. | "Health Information" means individually identifiable information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and any individually identifiable health information that is derived or extrapolated from information about an individual's activities, or pattern of activities, from which a determination is made that the individual has a health condition or is taking a drug.<br><br>"Individually Identifiable Health Information" means any information, including demographic information collected from an individual, that: (1) is created or received by a Health Care Provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, and: (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. |
| In re BetterHelp Inc., FTC Docket No. C-4796 (Jul. 14, 2023) | Finalized order issued July 14, 2023. | Teletherapy platform BetterHelp deceived users by promising not to disclose personal health data beyond limited purposes, but users' personal information and health questionnaire data was shared with third-party advertisers. BetterHelp also used this health information to target consumers with advertisements for BetterHelp's counseling services and did | “Treatment Information” means individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of a consumer, including:<br>1. drug, prescription, and pharmacy information;<br>2. information concerning the consumer’s diagnosis;<br>3. information concerning the consumer’s |

| | | | |
|---|---|---|---|
| | | not have any limits for how third parties could use data for advertising. BetterHelp was fined $7.8 million. | use of, creation of an account associated with, or response to a question or questionnaire related to, a service or product offered by Respondent or through one of any of Respondent's online properties, services, or mobile applications;<br>4. information concerning medical- or health-related purchases;<br>5. information concerning the past, present, or future payment for the provision of health care to the consumer; or<br>6. information derived or extrapolated from any of (1)-(5) above (e.g., proxy, derivative, inferred, emergent, or algorithmic data). |
| Easy Healthcare Co., FTC Docket No. 1:23-cv-3107 (May 17, 2023) | Finalized order issued June 26, 2023. | Fertility app Premom (developed by Easy Healthcare) violated the Health Breach Notification Rule and deceived users by promising to get users' consent before sharing health information with third parties and to only collect non-identifiable data for analytics and advertising, but the app disclosed highly sensitive health data (sexual and reproductive health, parental and pregnancy status, physical health conditions, etc.) through the integration of SDKs from AppsFlyer, Google, and other third party providers. Data shared with third-party SDKs included non-resettable mobile identifiers and precise geolocation information. Easy Healthcare was fined $200,000 by the FTC and Connecticut, DC, and Oregon. | "Health Information" means medical records and other individually identifiable information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. It includes, but is not limited to, information concerning fertility, menstruation, sexual activity, pregnancy, and childbirth. It also includes any individually identifiable information relating to health that is derived or extrapolated from non- health information (e.g., proxy, derivative, inferred, emergent, or algorithmic data). Health Information includes PHR Identifiable Health Information, as defined below, and Health Information associated with Personal Information, as defined below.<br><br>"Individually Identifiable Health Information" means any information, including demographic information, collected from an individual that: (1) is created or received by a Health Care Provider, health plan, employer, or health care clearinghouse; and (2) relates |


1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org