



**NAI Legal and
Regulatory Analysis:**

Sensitive Health Information

SEPTEMBER 2023

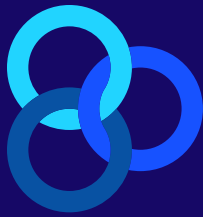


TABLE OF CONTENTS

I. Introduction.....	3
II. The Expanding Legal and Regulatory Landscape.....	5
A. The Federal Trade Commission (FTC) – Section 5 and HBNR Authority.....	5
B. The Department of Health and Human Services (HHS) – HIPAA Privacy Rule Authority	14
C. State Privacy Laws.....	16
III. Practical Takeaways for the Digital Advertising Industry and Beyond.....	19
IV. Appendix.....	25
A. Defining “Sensitive Health” Information Across the U.S.	25
B. Requirements for Obtaining Consumer Permission Across the U.S.	35
C. Other Obligations Associated with Processing Sensitive Health Information	43
D. Business Associate Agreement Requirements	43

I. Introduction

Health-related advertising has been around nearly as long as advertising itself. As early as the mid-1800s, drug manufacturers began advertising medications to consumers, connecting individuals with genuinely helpful information about products aimed at improving their health.¹ While much has changed in the intervening years, health related advertising still plays an extremely valuable role in American society for consumers and industry alike. At the same time, collecting and processing sensitive health information for targeted advertising can be problematic when proper safeguards fail to be implemented. However, through careful understanding of new legal requirements and thorough review of internal data collection and use, there remain viable paths for companies to engage in health-related targeted advertising, while protecting and respecting the rights and safety of consumers they serve.

In light of the 2022 U.S. Supreme Court decision, *Dobbs v. Jackson Women's Health Clinic*, which eliminated the constitutional right to an abortion, many are concerned that a broad swath of online information could be used to indicate a consumer's health status and ultimately fall into the hands of prosecutors in states where abortions are newly illegal. To this end, state and federal regulators have publicly committed to enforcing against these privacy failures to their fullest extent. Now more than ever, it is essential for participants in the digital advertising industry and beyond to be keyed into legal and regulatory updates, and to understand exactly how they apply to their business practices.


As a result of the emphasis placed on safeguarding online consumer health-related data, the regulatory landscape in this area has rapidly evolved at a pace difficult for companies of all sizes to maintain. Over the last 18 months, new state privacy laws, federal enforcement actions, and associated guidance have created significant new conclusions regarding how sensitive health data should be defined and treated. These conclusions will ultimately change the way members of the digital advertising industry approach data collection and use – even for those that work with information that has not traditionally been considered “sensitive” or “health-related.”

At the national level, the Federal Trade Commission (“FTC” or “Commission”) has primarily used its Section 5 Unfair and Deceptive Acts or Practices (“UDAP”) authority to regulate the collection and use of sensitive health data. The Commission has also exercised its authority pursuant to the Health Breach Notification Rule (“HBNR” or “Rule”), ensuring breaches of unsecured personal health records (“PHR”) are properly disclosed. In 2023, the Commission brought numerous health-related cases pursuant to these authorities that offer new interpretations regarding how to define sensitive health data, and the types of practices that may bring companies into the Commission's regulatory cross hairs. Also at the federal level, the Department of Health and Human Services (“HHS”), which has authority to enforce the Health Insurance Portability and Accountability Act (“HIPAA”), recently published a Bulletin expanding the interpretation of what constitutes HIPAA covered health information online – an explicit warning to covered entities that employ third party advertising technologies on their websites. Private litigants are also

1. The History of Drug Advertising, Weill Cornell Medicine's Samuel J. Wood Library (Apr. 2021).

monitoring this changing landscape as evidenced by a number of lawsuits filed against hospitals and other covered entities, claiming impermissible disclosure of protected health information (“PHI”) through the use of technologies like cookies, web beacons, and pixels.

At the state level, members of the digital advertising industry also need to be cognizant of new comprehensive and health-specific privacy laws – most of which require covered businesses to obtain affirmative consent before processing sensitive personal information relating to an individual’s health. In 2023, the number of U.S. state comprehensive privacy laws doubled. Additionally, three States adopted health-specific privacy laws that impose novel consent requirements for broadly defined “consumer health data.” This “patchwork” of state laws creates significant challenges for companies subject to compliance in multiple states, where the definitions and requirements associated with various types and uses of data – including sensitive data – often vary. While enforcement actions specific to sensitive health data have not yet arisen at the state level, regulators have indicated this is a priority area, and companies should be prepared to begin obtaining consent to use most health-related identifiable information.



All NAI members should consult with counsel to determine how these legal requirements apply to their specific business activities.

The legal and regulatory trends assessed in this resource demonstrate that U.S. regulators are committed to carefully investigating data collection across websites and apps, especially data that pertains to a consumer’s health. As scrutiny increases at the state and federal level, companies that wish to continue operating in the health space must understand their legal obligations, be equipped to make informed decisions about their data collection and sharing practices, and work closely with their vendors and partners to ensure they are doing the same. This resource explains recent legal and regulatory developments and enforcement, as well as provides compliance considerations for companies in the digital advertising industry and beyond. While it provides general explanations of the impact of certain laws and regulations on business practices, it does not constitute legal advice. All NAI members should consult with counsel to determine how these legal requirements apply to their specific business activities.

II. The Expanding Legal and Regulatory Landscape

For companies operating in the digital advertising industry and working with potentially health-related information, it is critical to be aware of multiple recent legal and regulatory developments at the federal and state level that could apply to common business practices. Largely, policy makers and regulators are adopting an increasingly

Policy makers and regulators are adopting an increasingly broad approach to defining ‘sensitive health data.’

broad approach to defining “sensitive health data,” including through the concept of inferences made by combining one or more points of data to reveal information about a consumer’s health. In light of recent changes, commonly employed uses of data and business practices that have traditionally been considered non-sensitive may now require heightened consumer notice and consent, or may be off limits altogether. For this reason, it is more important than ever for companies to understand obligations and develop a sound approach to remaining compliant.

Although this area of the law continues to evolve almost daily, and many requirements remain unclear, digital advertising companies must recognize the changing legal environment and assess how these developments affect their business practices and future strategy. This section explains the scope of sensitive health data across the various U.S. legal regimes, and accompanying requirements that should be considered in one’s risk analysis.

A. The Federal Trade Commission

The FTC is the chief consumer protection authority in the United States and the de facto national authority on privacy law in the absence of comprehensive federal legislation. With respect to sensitive health information, the Commission’s primary legal tools are its Section 5 and Health Breach Notification Rule authorities.

The Commission’s principal tool for enforcing against privacy harms associated with sensitive health data stems from Section 5 of the FTC Act, which outlaws “unfair or deceptive acts or practices in or affecting commerce.”² The FTC’s Section 5 authority is extremely broad, and encompasses virtually all business-related activities, with certain exceptions.³ Therefore, anyone operating a business for profit in the U.S., including every member of the third-party digital

2. [15 U.S.C. § 45\(a\)\(1\)](#).

3. See *Fed. Trade Comm’n v. AT&T Mobility LLC*, 883 F.3d 848, 863-64 (9th Cir. 2018) (Section 5 explicitly bars the FTC from regulating “common carriers” unless enforcement actions apply to a common carriers’ non-common carriage activities); 49 U.S.C. §1371 (2018) (Air carriers are exempt from the jurisdiction of the FTC); 49 U.S.C. § 41712 (DOT retains jurisdiction to review all cooperative arrangements between domestic and international airlines for unfair methods of competition); *but see Fed. Trade Comm’n v. Motion Picture Advertising Service Co.*, 344 U.S. 392, 394-95 (1953) (“Congress advisedly left the concept [of unfair methods of competition] flexible”); *American Airlines, Inc. v. North American Airlines, Inc.*, 351 U.S. 79, 85 (1956) (“[u]nfair or deceptive practices or unfair methods of competition . . . are broader concepts than the common-law idea of unfair competition”).

advertising industry as well as HIPAA-covered entities, must abide by the FTC Act and refrain from committing unfair or deceptive acts or practices.

In order to determine whether an act or practice is “unfair,” the Commission must demonstrate the practice 1) causes or is likely to cause substantial injury to consumers, 2) is not reasonably avoidable by consumers, and 3) is not outweighed by countervailing benefits to consumers or to competition.⁴ Some common examples of “unfair” practices include retroactive changes to privacy policies,⁵ the use of “dark patterns”,⁶ sale of sensitive data without consent,⁷ and inadequate data security practices.⁸ Of late, the FTC has prioritized actions against companies unfairly handling sensitive data without obtaining affirmative express consumer consent.⁹

Before collecting, using, or sharing sensitive personal information, companies must obtain affirmative express consent.

The Commission has long maintained that before collecting, using, or sharing sensitive personal information, companies must obtain affirmative express consent.¹⁰ This consent must be a “freely given, specific, informed, and unambiguous indication of an individual consumer’s wishes demonstrating agreement by the individual, such as by a clear affirmative action,” and requires a clear and conspicuous disclosure of 1) the categories of information to be collected, 2) the specific purpose for the collection, use, or disclosure, 3) the names or categories of third parties that collect the information or to whom the information is disclosed, 4) an easily accessible means for a consumer to withdraw consent, and 5) any potential limitations to the consumer’s ability to withdraw consent.¹¹ The FTC has suggested that affirmative express consent requires a disclosure that is separate and distinct from a company’s more general privacy policy and cannot

4. Fed. Trade Comm’n, [A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority](#) (May 2021).

5. See Proposed Decision and Order, *In the Matter of, Facebook, Inc.*, Docket No. C-4365 (May 3, 2023).

6. See Fed. Trade Comm’n v. Vonage Holdings Corp., 2022 WL 16833021 (D.N.J. 2022); see also FTC Press Release, FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers (Sept. 15, 2022); see also FTC Staff Report, Bringing Dark Patterns to Light (Sept. 2022); see also The NAI, Best Practices for User Choice and Transparency (May 10, 2022).

7. See [In the Matter of, BetterHelp, Inc.](#), Decision and Order (March 2, 2023).

8. Fed. Trade Comm’n v. Wyndham Worldwide Corporation, 799 F.3d 236 (3rd Cir. 2015); *LabMD, Inc., v. Fed. Trade Comm’n*, 894 F.3d 1221 (11th Cir. 2018); Decision and Order, *In the Matter of, Drizly, LLC.*, 2022 WL 16635415, No. 202-3185, (October 24, 2022).

9. See [In the Matter of BetterHelp, Inc.](#), Complaint (Mar. 2, 2023); [U.S. v. GoodRx Holdings, Inc.](#), Complaint (Feb. 1, 2023).

10. FTC Staff Report, [Self-Regulatory Principles for Online Behavioral Advertising](#) at 47 (Feb. 2009).

11. [In the Matter of, BetterHelp, Inc.](#), Decision and Order, (March 2, 2023).

include elements such as pre-checked boxes or pre-filled forms.¹²

While there is neither a statutory definition of sensitive personal information, nor has the Commission provided an explicit definition for the term, recent enforcement actions and official Commission publications are instructive as to the types of personal information the Commission considers sensitive. At a minimum, the Commission has stated that personal information such as children’s data, financial and health information, Social Security numbers, and certain geolocation data is sensitive and thus, requires affirmative express consent.¹³

As indicated in its complaint against GoodRx,

“health information” may include information that “could be linked to (or used to infer information about) chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, sexual orientation, and other highly sensitive and personal information.”¹⁴ However, this list is not exhaustive and the FTC has indicated that defining sensitive information “is complex and may often depend on the context.”¹⁵

‘Health information’ may include information that ‘could be linked to (or used to infer information about) chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, sexual orientation, and other highly sensitive and personal information.

Per the Commission’s recent actions, information such as email and IP addresses alone could be sensitive and thus, would require express affirmative consent in instances where “disclosure of that information to a third party would *implicitly* disclose ... the consumer’s health information[,]” regardless as to whether a particular company is subject to HIPAA, or where it sits in the larger data flow.¹⁶ In the case against BetterHelp, for example, the Commission claimed this implicit disclosure occurred because the company only offered one service – online mental health counseling. Therefore, consumers that provided their email to sign up for an account were

12. FTC Staff Report, [Self-Regulatory Principles for Online Behavioral Advertising](#) at 44, N77 (Feb. 2009) (“pre-checked boxes or disclosures that are buried in a privacy policy or a uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer’s ‘affirmative express consent.’”)

13. Fed. Trade Comm’n, [Protecting Consumer Privacy In An Era of Rapid Change](#) at 47, N214 (Mar. 2012).

14. [U.S. v. GoodRx Holdings, Inc.](#), Complaint at 4 (Feb. 1, 2023).

15. FTC Staff Report, [Self-Regulatory Principles for Online Behavioral Advertising](#) at 44 (Feb., 2009).

16. [In the Matter of BetterHelp, Inc.](#), Complaint at 1-2 (Mar. 2, 2023) (“For example, because Respondent obtained a consumer’s email address only when the consumer took affirmative steps to utilize the Service, Respondent’s disclosure of this information would identify the consumer as associated with seeking and/or receiving mental health treatment. Similarly, Respondent’s disclosure that a consumer took affirmative steps to sign up for the Service (such as by filling out Respondent’s intake questionnaire for the Service or becoming a paying user), along with an identifier (for example, an IP address), would disclose the consumer’s seeking of mental health treatment via the Service.”).

presumed to be seeking mental health care, implicitly disclosing sensitive information. Based on the Commission's approach in its complaint against BetterHelp and others, companies must take a broad approach to defining sensitive information. If personal information sufficiently connects a user to a health condition or treatments/interest in that condition or treatment, that information is likely sensitive health data for purposes of the Commission's unfairness authority.

If personal information sufficiently connects a user to a health condition or treatments/ interest in that condition or treatment , that information is likely sensitive health data for purposes of the Commission's unfairness authority.

In addition to its unfairness authority, the FTC also has the authority to bring separate claims for deceptive acts and practices pursuant to Section 5. To do so, the agency relies on a three-pronged test to determine if a practice meets the standard of "deception" – 1) there must be a representation, omission, or practice that is likely to mislead the consumer; 2) the representation must be one a reasonable consumer would consider misleading; and 3) the representation, omission, or practice must be material.¹⁷ Traditional deception claims in the privacy and security space have often focused on inconsistencies between companies' data handling practices and public facing privacy notices and marketing materials.¹⁸ Recently, the Commission has also brought deception counts in instances where companies handling health-related consumer information purport to be HIPAA compliant, when in fact they are not covered entities for purposes of the law and have not engaged in a formal review for compliance.¹⁹

Apart from Section 5, the FTC also regulates sensitive non-HIPAA health data through the HBNR – a 2009 law that requires certain entities to make disclosures to consumers, regulators, and occasionally the media if they experience an unauthorized disclosure or breach of unsecured, individually identifiable electronic personal health records.²⁰

The HBNR applies to entities that maintain or interact with "personal health records" ("PHR") – "electronic record[s] of PHR identifiable health information on an individual that can be drawn from multiple sources and that [are] managed, shared, and controlled by or primarily for the individual."²¹ According to the Commission, PHR identifiable information includes location data, user input data, and medication information. Based on enforcement actions and the

17. [Letter from James C. Miller, Chairman, Federal Trade Commission, to the Hon. John D. Dingell, Member of Congress](#) (Oct. 14, 1983) (hereinafter "Policy Statement on Deception").

18. Fed. Trade Comm'n, [Privacy and Security Enforcement](#) (last visited Aug. 11, 2023).

19. See *In the Matter of BetterHelp, Inc.*, Complaint (Mar. 2, 2023); *U.S. v. GoodRx Holdings, Inc.*, Complaint (Feb. 1, 2023).

20. [Health Breach Notification Rule](#), 74 FR 42961 (finalized Aug. 25, 2009) (codified at 16 CFR Part 318).

21. 16 C.F.R. § 318.2(d); For example, "if you develop a health app that collects information from consumers and can sync with a consumer's fitness tracker, you're probably a vendor of personal health records ..." Fed. Trade Comm'n, [Complying with FTC's Health Breach Notification Rule](#) (Jan. 2022).

Commission's recently proposed modifications to the Rule, it is plausible that the FTC may consider information regarding a consumer's mere interest in a health condition as a PHR when combined with other information.

In the event of a breach of an unsecured PHR, vendors of PHR²² and PHR related entities²³ are required to notify affected individuals, the FTC, and in some cases, the media.²⁴ Third party service providers²⁵ are only required to notify such vendors or entities in the event they experience a breach, so that the vendors or entities can then make the required disclosures.²⁶ While it is unlikely that a third party digital advertising company would be considered a vendor or related entity, the Rule is still relevant to them.²⁷ Depending on the Commission's forthcoming final revised Rule, a digital advertising company providing analytics or attribution services to vendors or related entities could be considered a third party under the Rule to the extent it accesses PHR identifiable health information and would be required to comply with the HBNR as well.

It is plausible that the FTC may consider information regarding a consumer's mere interest in a health condition as a PHR when combined with other information.

22. 16 C.F.R. § 318.2(j) ("Vendor of personal health records means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.").

23. 16 C.F.R. § 318.2(f) ("PHR related entity means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) Offers products or services through the Web site of a vendor of personal health records; (2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or (3) Accesses information in a personal health record or sends information to a personal health record.").

24. 16 C.F.R. §§ 318.3 (a)(1)-(2) (Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.).

25. 16 C.F.R. § 318.2(h) ("Third party service provider means an entity that: (1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.").

26. 16 C.F.R. § 318.3(b).

27. 16 C.F.R. § 318.2(j) ("Vendor of personal health records means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.").

In its 2021 Policy Statement, the FTC significantly expanded the scope of the Rule by clarifying that health applications and connected devices, such as menstrual cycle trackers and fitness wearables are covered by the HBNR. Further, the Commission asserted that “breaches” are “not limited to cybersecurity intrusions or nefarious behavior[,]” and that “[i]ncidents of unauthorized access, including sharing of covered information without an individual’s authorization for advertising, triggers notification obligations under the Rule.”²⁸ Unauthorized access does not constitute a “breach” if the information at hand cannot reasonably identify an individual (e.g., if the information is properly de-identified). The FTC views device and advertising identifiers as reasonably identifiable to an individual.²⁹

[I]ncidents of unauthorized access, including sharing of covered information without an individual’s authorization for advertising, triggers notification obligations under the Rule.

In May 2023, the Commission voted to initiate a Proposed Rulemaking, seeking to update the HBNR to provide clarity regarding the scope of regulated entities, and better align definitions with the Commission’s recent Policy Statement and enforcement actions.³⁰ Based on the proposed changes to the Rule, the Commission seems focused not only on new types of consumer health information outside of the scope of HIPAA, such as heart rate and temperature information collected through a sensor, but also other forms of data, such as location data that could be combined with other health information in a personal health record. Based on the FTC’s expanded interpretation of breach and PHR identifiable information, and the recent uptick in enforcement actions, more companies that provide purely analytics services may be pulled into the scope of the Rule, and must be aware of the various requirements that come along with this designation.

The Commission brought three health-related enforcement actions in the Spring of 2023, employing both its Section 5 and HBNR authority. While all three actions were brought against consumer facing companies that provide traditionally “health-related services,” the implications are potentially far reaching, and provide valuable takeaways for third party digital advertising companies. As the Commission has indicated, while these actions did not deal with this concept directly, even downstream companies can face liability when receiving sensitive health information from partners that did not obtain proper consent before disclosure.³¹

28. [FTC’s Policy Statement on Health Breach Notification Rule](#) (Sept. 2021) (hereinafter “HBNR Policy Statement”).

29. Fed. Trade Comm’n, [Complying with FTC’s Health Breach Notification Rule](#) (Jan. 2022).

30. NPRM at 37822.

31. Elisa Jillson, [Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases](#), The Fed. Trade Comm’n (Jul. 25, 2023).



U.S. v. GoodRx Holdings – As a “consumer-focused digital healthcare platform” connecting consumers with prescription discounts, GoodRx “advertises, distributes, and sells health-related products and services directly to consumers, including purported prescription medication discount products[.]”³²

To facilitate these services, GoodRx collects information from its users, including name, phone number, email address, prescription name, dose, form, and quantity, medication purchase history, location, IP address, and advertising identifiers.³³ In its complaint, the FTC alleged GoodRx shared this information with third-party advertising platforms via tracking pixels, and then used these tracking tools to facilitate analytics and ad targeting, including to create segments based on health condition or medication use. According to the Commission, the company did so without obtaining consumer consent. From 2017 forward, GoodRx’s public facing privacy policy promised it would only share this information “with limited third parties and only for limited purposes; that it would restrict third parties’ use of such information; and that it would never share personal health information with advertisers or other third parties.”³⁴ Its website also displayed a HIPAA compliance seal, indicating that it followed the law’s requirements, even though the company was/is not a covered entity.

The Commission charged GoodRx with multiple deception and unfairness counts, and one count of violating the HBNR. The FTC asserted the information GoodRx collected was sensitive health data, as it “revealed extremely intimate and sensitive details about GoodRx users that could be linked to (or used to infer information about) chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, sexual orientation, and other highly sensitive and personal information.”³⁵ By sharing this information with third parties for advertising purposes without affirmative express consent, and failing to contractually limit third party use, the FTC alleged that GoodRx committed an unfair trade practice. Further, the Commission opined, this sharing was contrary to the company’s website disclosures and privacy policy, deceiving consumers. The Commission also said that as a Vendor of PHR, GoodRx’s website and mobile apps were “electronic records of PHR identifiable health information that are capable of drawing information from multiple sources,” and that the company violated the HBNR when it shared this information with third parties and failed to notify the proper entities.³⁶

32. [U.S. v. GoodRx Holdings, Inc.](#), Complaint at 4 (Feb. 1, 2023).

33. *Id.* at 11.

34. *Id.* at 2.

35. *Id.* at 4.

36. *Id.* at 25.



In the Matter of BetterHelp – BetterHelp is an online mental health counseling service that matches users with therapists. To use the service, BetterHelp requires consumers to provide their email and answer a detailed intake questionnaire about their mental and physical medical history.³⁷ BetterHelp collects users’ names, email addresses, phone numbers, credit card information, IP addresses, ages, sexuality, medication use, religion, and therapy history. In its complaint against the company, the FTC alleged BetterHelp shared this information with third party advertising platforms via tracking pixels to facilitate retargeting and analytics, and to create custom audiences without obtaining user consent.³⁸ BetterHelp’s consumer disclosures repeatedly promised the limited sharing of personal information for actions related to its services, and never mentioned this information’s use for advertising purposes. BetterHelp also displayed a HIPAA seal on its website, indicating its compliance with the law when, like GoodRx, the company was not a covered entity.³⁹

As a result, the Commission brought multiple unfairness and deception counts against the company using its Section 5 authority. It claimed that BetterHelp’s false representations regarding its data sharing practices and failure to disclose the fact that health information was being shared with third parties were materially deceptive, and misled consumers about the safety of their sensitive information. The Commission also determined BetterHelp’s use of the HIPAA seal was deceptive, as its data handling practices were not subject to review for compliance, and many of BetterHelp’s therapists were not subject to HIPAA.

Most notable in this case was the use of the Commission’s unfairness authority. In addition to reaffirming the need to obtain affirmative express consent when collecting, using and disclosing sensitive information, the FTC further expanded its interpretation of what constitutes sensitive personal health information, and thus, when this consent must be obtained. The Commission determined that because BetterHelp only collected emails from consumers who signed up for therapy services, the sharing of the emails alone constituted disclosure of health information without express affirmative consent, as the email address “implicitly disclose[d] the consumer’s interest in or use of the Service ...”⁴⁰ What is more, hashing those emails *did not* eliminate their sensitivity, as

37. [In the Matter of BetterHelp, Inc.](#), Complaint at 2 (Mar. 2, 2023).

38. *Id.* at 10.

39. *Id.* at 14.

40. *Id.* at 1.

the hashing was meant only to protect against bad actors, and the emails were shared with entities that had the ability to unhash or match the emails to identities.⁴¹



U.S. v. Easy Healthcare Corporation – “Premom” is a free ovulation and fertility tracking app developed by Easy Healthcare Corporation. The app collects information about consumers, “including dates of menstrual cycles, temperatures, pregnancy and fertility status, whether and when pregnancies started and ended, weight, progesterone and other hormone results, ... pregnancy-related symptoms[,]” user location, advertising IDs, and non-resettable hardware IDs.⁴² The Premom app shared this information, along with custom app events, with third parties through the use of software development kits (“SDKs”) for marketing and analytics purposes. Premom’s contracts with their third party partners did not limit the partners’ use of the consumer data, permitting them to track users across the web utilizing non-resettable IDs. Like GoodRx and BetterHelp, Premom’s privacy disclosures repeatedly affirmed this data would only be used for internal statistical and marketing purposes, and that it would only share *unidentifiable* data with third parties.⁴³

The Commission brought multiple unfairness and deception counts against Premom, and one count for violating the HBNR. Contrary to its public disclosures, the Commission asserted Premom misrepresented its data handling practices, unfairly shared sensitive health data with third parties without the consent of consumers, and failed to contractually prohibit these third parties from using the data for their own purposes. The FTC claimed that Premom also violated the HBNR because it failed to notify relevant parties of the disclosure of unsecured personal health records, which included user uploaded ovulation test results and information collected from Bluetooth devices such as connected thermometers.

41. *Id.* at 10-11 (“Although Respondent ‘hashed’ Visitors’ and Users’ email addresses (i.e., converted the email addresses into a sequence of letters and numbers through a cryptographic tool) before disclosing them to third parties, the hashing was not meant to conceal the Visitors’ and Users’ identities from Facebook or the other recipient third parties. Rather, the hashing was done merely to hide the email addresses from a bad actor in the event of a security breach. In fact, Respondent knew that third parties such as Facebook were able to, and in fact would, effectively undo the hashing and reveal the email addresses of those Visitors and Users with accounts on the respective third parties’ platforms, which is how Facebook matched these email addresses with Facebook user IDs. Indeed, Facebook’s standard terms of service, to which Respondent agreed, explained that Facebook would use hashed email addresses it received from Respondent to match Visitors and Users with their Facebook user IDs for advertising purposes, among other things. Thus, Respondent knew that by sending these lists of Visitors’ and Users’ email addresses to third parties, it was telling these third parties which of their users were seeking or in therapy through the Service.”).

42. [U.S. v. Easy Healthcare Corporation](#), Complaint at 6 (May 2023).

43. *Id.* at 7.

B. The U.S. Department of Health and Human Services (HHS) – HIPAA Privacy Rule Authority

The U.S. Department of Health and Human Services (“HHS”) has statutory authority to promulgate implementing rules for the Health Insurance Portability and Accountability Act (“HIPAA”) of 1996.⁴⁴ While members of the advertising technology industry would not be considered traditional “covered entities” under the law, a recently issued HHS Bulletin suggests that, in some cases, these companies could be considered business associates and may be asked to sign data handling and security agreements by their covered entity data sharing partners.

The HIPAA Privacy Rule (the “Rule”) generally prohibits covered entities⁴⁵ such as hospitals and health care providers that transmit health information in electronic form from sharing “protected health information” (“PHI”)⁴⁶ without proper consumer authorization. However, the Rule allows covered entities to share PHI with “business associates” for certain uses, predefined through an agreement between the two known as a “business associate agreement.”⁴⁷ While a member of the digital advertising industry would likely never be considered a covered entity for purposes of HIPAA, they are more likely to be considered business associates – entities “that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide services to, a covered entity.”⁴⁸ Business associates include companies that access PHI in the course of providing analytic or data aggregation services on the websites of covered entities.

In a December 2022 Bulletin, HHS warned that common technologies such as cookies, web beacons, tracking pixels, session replay scripts, and fingerprinting scripts used by covered entities to collect and analyze the way consumers interact with their websites may collect PHI if the information relates to the individual’s “past, present, or future health or health care or payment for care.”⁴⁹ On user-authenticated web pages (e.g., a page where a user had to log in in order to

44. [Health Insurance Portability and Accountability Act of 1996](#) (HIPAA), 45 C.F.R. Part 160, 62, and 64.

45. 45 CFR § 160.103 (“Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”).

46. *Id.* (“individually identifiable health information that . . . is created or received by a [covered entity]; and 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.”).

47. *Id.* (“Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.”)

48. U.S. Dep’t of Health and Human Serv., [Business Associates](#) (last visited Aug. 11, 2023).

49. U.S. Dep’t of Health and Human Serv., [Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates](#) (Dec.1, 2022).

make an appointment with their physician or view test results, etc.), the Bulletin says that any tracking technology is generally considered to have access to PHI.⁵⁰

Further, while use of these technologies on a covered entity's non-authenticated web page usually do not have access to PHI, the Bulletin suggests that in certain instances, depending on the content and specificity of the web page (e.g., pregnancy, miscarriage, etc.), identifiable information such as an IP address may be considered PHI if it sufficiently associates the user with a medical condition.⁵¹ When covered entities

engage third-party companies to operate these technologies on their sites, or share their own information with the third-party for analytics, the third-party is considered a business associate, and the covered entity is considered to have committed an impermissible disclosure by sharing PHI with the third party if no business associate agreement exists between the two.⁵² In July 2023, HHS and the FTC issued another similar joint warning to hospital systems and telehealth providers, reiterating that third party analytics technologies may collect sensitive consumer health information regulated by both agencies, and emphasizing the responsibilities of actors on both sides of a data transaction.⁵³

The result of the dual warnings from the HHS and FTC is a broader interpretation of what constitutes HIPAA-protected PHI, and increased scenarios where a third party advertising

Identifiable information such as an IP address may be considered PHI if it sufficiently associates the user with a medical condition.

Common technologies such as cookies, web beacons, tracking pixels, session replay scripts, and fingerprinting scripts used by covered entities to collect and analyze the way consumers interact with their websites may collect PHI if the information relates to the individual's 'past, present, or future health or health care or payment for care.'

technology vendor could be considered a business associate (even when their relationship has not been formally recognized as such). Consequently, third party digital advertising companies operating tracking pixels on the websites of covered

50. *Id.*

51. *Id.* ("Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.")

52. *Id.* ("For example, if an individual makes an appointment through the website of a covered health clinic²⁸ for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.")

53. Fed. Trade Comm'n, [FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies](#) (July 20, 2023).

entities may begin receiving requests to sign BAAs to prevent unauthorized disclosure of PHI—which can include substantial obligations and significant restrictions on data use.⁵⁴ Based on the sheer number of covered entities hosting third-party analytics technologies,⁵⁵ and the increased scrutiny on their use, it is imperative that companies offering these services be aware of situations where they may be operating as a business associate, even on non-authenticated web pages. Companies should understand and carefully consider their potential obligations should they be asked to sign a business associate agreement, and be aware of instances where they can refuse to sign or push back on the requests of covered entities.

C. State Privacy Laws

In the absence of a federal comprehensive privacy law, U.S. states have taken it upon themselves to regulate consumer privacy in their respective jurisdictions and consequently, to regulate sensitive consumer health information not covered by HIPAA or another preemptive law. As of this resource's publication, 12 states have passed comprehensive privacy laws and dozens more are poised to join their ranks in the coming months and years.

While only Connecticut's comprehensive privacy law explicitly defines "health information" (added through amendment in 2023), every law contemplates a distinct category of personal information that should be considered "sensitive" that includes, to some extent, information pertaining to a consumer's health. The concept of sensitive information and the level of consent required to use it varies widely from jurisdiction to jurisdiction, leaving many companies subject

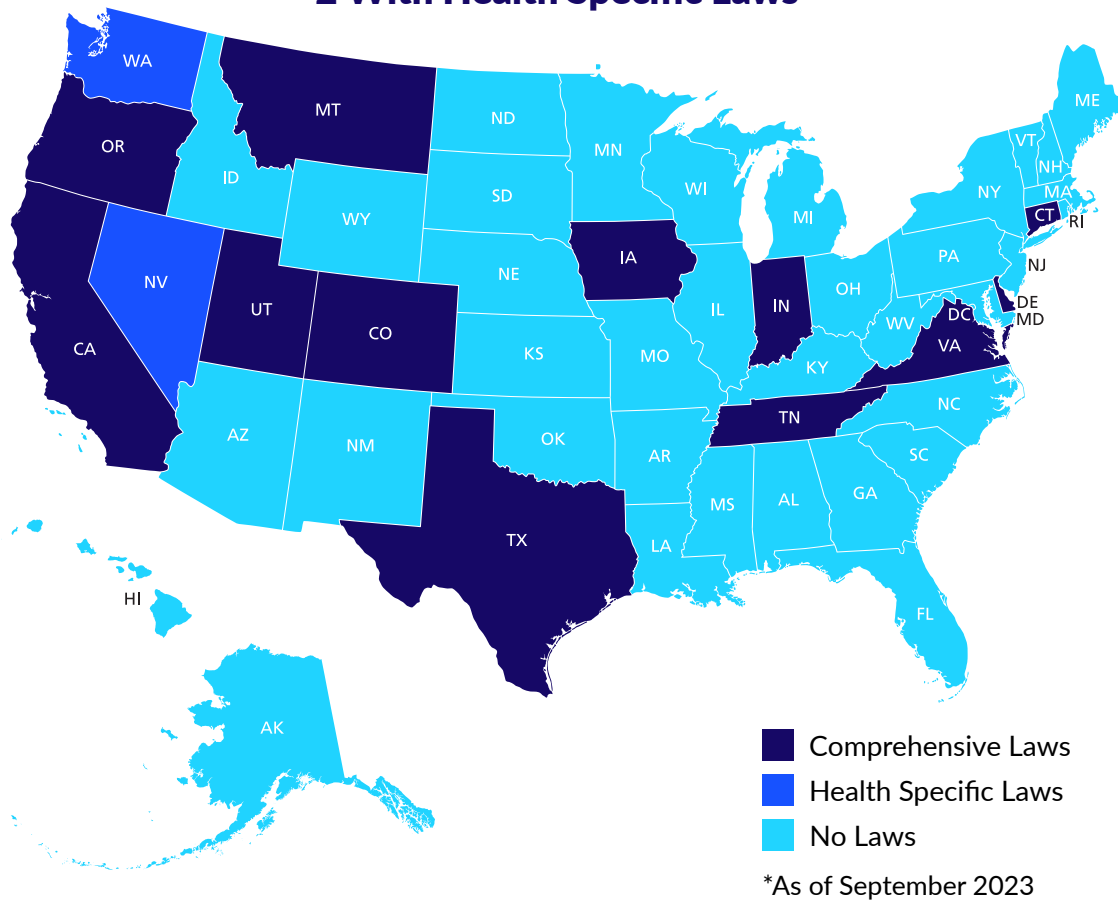
54. U.S. Dep't of Health and Human Serv., [Business Associate Contracts](#) (Jan. 25, 2013), ("A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.")

55. Ari B. Friedman et al., [Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals](#), *Health Affairs* Vol. 42, No.4 (April 2023).

to compliance in multiple states uncertain about how to achieve it.

The varying approaches to sensitive health data across the states are further complicated by “sensitive inferences” – the concept that information typically considered “non-sensitive” could in fact be captured by the definition of sensitive data if used to infer or reveal a health condition or diagnosis, such as pregnancy or asthma. For example, “[w]hile web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, infers an individual’s sexual orientation is considered Sensitive Data[.]”⁵⁶ Currently every state law except Iowa’s uses language such as “infers” or “reveals” in their respective definitions of sensitive information. In addition, California explicitly defines “inference” and Colorado’s implementing regulations define sensitive inferences and specifically explain they are subject to the same consent requirements as sensitive information more generally.⁵⁷

12 States With Comprehensive Laws, 2 With Health Specific Laws



56. 4 CCR § 904-3-2.02.

57. Cal. Civ. Code § 1798.140(r) (“Infer’ or ‘inference’ means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.”); 4 CCR § 904-3-2.02 (“Sensitive Data Inference’ or ‘Sensitive Data Inferences’ means inferences made by a Controller

In addition, the national focus on reproductive health information post-Dobbs has led many states to introduce health-specific privacy bills in the 2023 session that purport to fill the gaps left by HIPAA and go beyond the protections offered by existing laws. Most notable among these is the first such law enacted, Washington state’s “My Health My Data Act” (“MHMD”).⁵⁸ As of August 2023, Nevada also enacted a law modeled closely on MHMD, and Connecticut passed an amendment to its comprehensive privacy law that includes core pieces of that statute as well.

MHMD restricts the collection, sharing, and sale of “consumer health data” – broadly defined to include “personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status[,]” including “precise location information that could reasonably indicate a consumer’s attempt to acquire or receive health services or [supplies]” and information derived or extrapolated from non-health information.⁵⁹ “Health care services” as used in this definition include “any service provided to a person to assess, measure, improve, or learn about a person’s mental or physical health . . .”⁶⁰ The law requires separate opt-in consent to both collect and share this consumer health data, and “valid authorization” from consumers before selling an individual’s consumer health data.⁶¹

Taken together, these broadly defined terms create tremendous uncertainty about the scope of MHMD’s application, and the kinds of information that could identify a consumer’s health status. Compounding the business challenges created by the ambiguous definitions and anticipated enforcement by the state Attorney General, MHMD also provides for enforcement through private action. Consequently, covered businesses operating in Washington need not only consider the potential of Attorney General enforcement, but also whether they might become targets of private suits.

In an attempt to combat the potential flurry of private actions based on unreasonably broad interpretations of the law and clarify potential ambiguities, the Washington Attorney General’s office released a guidance document in June 2023, addressing some common areas of confusion.⁶² Specifically, the Attorney General asserted that consumer health data should not be interpreted to include information regarding the purchase of toiletries such as deodorant, toilet paper or mouthwash. However, information from an app that tracks digestion or perspiration would be considered consumer health data. Although MHMD does not provide the Attorney General with formal rulemaking authority and thus, this guidance does not carry the force of law, the clarification is a helpful one. Notably, similar statutes passed in Nevada and Connecticut do not contain a private right of action.

58. The [“My Health, My Data” Act](#) (MHMD), Washington House Bill 1155 (2023).

59. *Id.* at §2(8).

60. *Id.* at §2(15).

61. *Id.* at §9.

62. WA State Office of the Attorney General, [Protecting Washingtonians’ Personal Health Data and Privacy](#) (last visited Aug. 11, 2023).

III. Practical Takeaways for Members of the Digital Advertising Industry and Beyond

The majority of the legal action related to sensitive health data has been reserved for companies who operate in the traditional “health space” – including healthcare provider websites and portals, wellness applications, fitness wearables, and online consumer services. However, in practice, the potential for liability spreads much further.

In a recent blog post, the FTC emphasized this, reminding companies that recipients of improperly disclosed sensitive health information may also face potential liability. Specifically, third party digital advertising companies, including a majority of NAI membership, should take stock of their data collection and handling practices and assess the potential applicability to their own organizations – even those companies whose business models do not fit squarely in the health space or do not work directly with traditional health data. In light of the increased attention to sensitive inferences, even non-health data has the potential to reveal sensitive attributes about consumers according to the regulatory bodies charged with enforcing the various governing laws in this area.



Recipients of improperly disclosed sensitive health information may also face potential liability.

For some, the national scrutiny of sensitive health data has raised questions as to whether health-related target advertising is still a viable business practice, or if they should avoid it completely in order to fend off regulators until legal conclusions become clearer. While this is a sure way to avoid liability in an area with little clarity, the result would be harmful for consumers and businesses who genuinely benefit from health-related targeted advertising. While the bottom line in the sensitive health data debate remains largely unsettled, there are many mitigating factors and best practices members of the digital advertising industry can and should take from recent enforcement action and regulatory guidance to help reduce potential liability and retain some of the lucrative and beneficial effects of health-related targeted advertising.

The following are general suggestions based on recent regulatory trends, not legal advice. The applicability and usefulness of each depends on the risk tolerance and business practices of individual companies. *The NAI encourages you to consult with outside counsel for more clarity on how these apply to your own organization, and how your organization should approach handling potential sensitive health information.*

- **Say what you do, do what you say, and be mindful of what you don't say**

A simple way for companies to avoid regulatory scrutiny begins with a strong and clear privacy policy that accurately reflects how sensitive health information is handled and shared. Throughout its complaints against GoodRx, BetterHelp, and Premom, the FTC repeatedly pointed to the fact that the companies' sensitive data handling practices were materially different from what they represented in their privacy policies and on their websites. Moreover, these companies also found themselves in regulatory hot water for material *omissions* as well. For this reason, the Commission has warned “[i]t's

crucial to disclose all material information to consumers about how you're using and disclosing their sensitive health information."⁶³ By reviewing internal practices, taking time to understand the breadth of what constitutes sensitive health information, communicating openly with other departments within an organization (including product and marketing), and making sure one's privacy policy accurately reflects business practices, companies can demonstrate they are responsible actors.

- **False or misleading compliance seals could lead to deception charges**

In its complaints against GoodRx and BetterHelp, the FTC noted that while the two companies were not HIPAA covered entities, both displayed HIPAA compliance seals on their sites, purporting to follow the law's requirements regarding PHI. The Commission indicated in those complaints and in a subsequent blog post that *only* HHS has the authority to determine HIPAA compliance, and that stating otherwise could deceive consumers.⁶⁴ While the Commission has not explicitly addressed other types of legal compliance certification programs, such as those created for state privacy laws, it is important to note that any misleading assertions about full compliance could create Section 5 liability for "both the certifier and the user of that false certification."⁶⁵ In addition to the FTC, companies displaying misleading compliance certificates could also face liability pursuant to state consumer protection statutes. To avoid this, companies should take care to ensure that even disclosures about voluntary compliance programs accurately reflect their legal obligations and status.

- **"Health" data is broadly defined and includes inferences**

As detailed in this resource, there are numerous legal regimes that govern the collection and use of sensitive health information for targeted advertising, each with their own unique approach for defining what this encompasses. "Health" information is no longer just about prescription records and medical diagnoses issued by doctors. It now represents a broad swath of data such as browsing history, purchase data, and location information that relates to a consumer's health status. Additionally, inferences represent a key element of the expanding approach to sensitive personal information, including instances where non-health information can be used to reveal an individual's mental or physical health condition or diagnosis.⁶⁶ Companies should therefore review their own interpretations and seek to ensure that they align with this broader approach.

The NAI Code of Conduct has long recognized that inferences that a user has, or is likely to have, certain sensitive health or medical conditions or treatments, including

63. Fed. Trade Comm'n, [Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases](#) (July 25, 2023).

64. *Id.*

65. *Id.*

66. *Id.*

cancer, mental health conditions, and sexually-transmitted diseases, should be treated as sensitive information, even when these inferences are made from traditionally nonsensitive information. However, current law is unclear as to where exactly this line is drawn, and when seemingly benign information could “reveal” a sensitive attribute about a consumer. The varying definitions and approaches to the kinds of information about a consumer’s health (e.g., an inference that a consumer has seasonal allergies versus an inference about a terminal disease) that should be considered sensitive further complicates this.

- **Ensure the sensitive health information you collect and receive is properly permissioned**

With an expanding definition of health information comes expanded instances where consumer consent is required. The FTC has made clear it expects companies collecting, sharing, or receiving sensitive health information to ensure affirmative express consent is obtained. In its recent blog post, the Commission emphasized that pursuant to Section 5, recipients have an obligation to “take steps (such as procedural and technical measures) to ensure [they] don’t engage in the unauthorized receipt, use, or onward disclosure of sensitive information.”⁶⁷ Most state laws similarly require consent before a company can process sensitive health information. California, Utah, and Iowa, are notable outliers, and only require companies to provide notice and an opportunity to opt-out before sensitive information is processed. However, due to the FTC’s approach, these outliers carry little weight, as the same information would require affirmative express consent at the federal level.

In addition, the Commission’s HBNR authority mandates covered companies collect consumer authorization before disclosing PHR identifiable health information that is part of a personal health record. Without such authorization, any sharing is a breach of security, triggering the Rule’s disclosure requirements. In a slightly different vein, the HIPAA Privacy Rule only permits the sharing of protected health information without authorization when a business associate agreement is in place. Health specific state privacy laws in Nevada and Washington take an analogous approach, requiring signed consumer authorization before the sale of consumer health information.

In addition to understanding when to obtain consent, the consent also needs to comport with relevant legal requirements. For example, the FTC has made clear that affirmative express consent requires more than just a pop-up notice, privacy policy, or link at the bottom of a sign up form – it involves disclosing the categories of information collected, the purpose of the collection, use or disclosure and to whom it is disclosed, and any potential limitations on the ability of the consumer to withdraw consent.⁶⁸ Further, in states with health specific privacy laws, “authorization” to

67. *Id.*

68. *In the Matter of, BetterHelp, Inc.*, Complaint, (March 2, 2023) (“Respondent failed to limit contractually how third parties could use consumers’ health information, instead merely agreeing to their stock contracts and terms.”).

sell consumer health data sets a higher bar than other approaches to consent, requiring a physical consumer signature and an expiration date.⁶⁹ For a list of consent requirements associated with the sensitive health information, please see the Appendix to this resource.

- **Commonly deployed technologies may trigger new obligations**

Common technologies used regularly to facilitate targeted advertising and analytics have been the subject of multiple administrative efforts and enforcement actions over the course of the last 18 months. Specifically, lawmakers and regulators have focused on instances where “pixels” – small pieces of invisible code that collect information about a consumer’s movements on a webpage – have been used to collect and share information that may amount to an inference about a consumer’s mental or physical health. For example, the FTC alleged third-party “tracking pixels” used by GoodRx and BetterHelp on their websites and apps collected information that revealed consumer interest in obtaining mental health services or purchasing certain medications, and consequently facilitated the sharing of sensitive health information. Similarly, HHS has publicly stated that tracking pixels used to “[connect] the individual to the regulated entity” are collecting HIPAA-covered PHI.

Despite the legal focus on “tracking” pixels, it is important to note that functionally, all pixels (retargeting, analytics, conversion, etc.) operate in the same manner, providing a third-party a “window” by which to obtain information about a consumer’s interactions on another website in the form of cookie IDs, IP addresses, and other commonly used identifiers. Differentiation between varying types of pixels, however, depends substantially on where and how they are used. For example, a conversion pixel placed on a check-out page could be used to determine how many consumers exposed to a specific advertisement actually purchased an item. Differently, retargeting pixels may be placed on a product page in order to serve a consumer an ad for the product the consumer viewed when they visit another site.

Notwithstanding the varying and often beneficial uses of pixels, it is not entirely clear to what extent regulators recognize these distinctions, labeling all pixels as “tracking pixels” and taking issue with the content of the webpage where a pixel is located, as opposed to its use. Additionally, much of the scrutiny associated with this technology also centers around their “surreptitious nature” and the fact that it is extremely difficult for consumers to know whether a pixel is present, or understand how to disable them. For these reasons, entities operating pixels on third-party sites should pay careful attention to the content of the webpages they serve, particularly taking stock of when consumer activity could indicate a mental or physical health condition or otherwise relate to an individual’s health. Similarly, publishers need also be cognizant of potential implications associated with hosting these technologies on health-related webpages, as they could face liability for sharing sensitive consumer information with third-parties. The FTC specifically has indicated that both ad techs

69. The [“My Health, My Data” Act \(MHMD\)](#), Washington House Bill 1155 § 9 (2023).

and publishers have a responsibility to ensure sensitive data that is shared between partners for the purposes discussed here is properly consented and is accompanied by proper safeguards, including contractual limits on onward use of information.

- **Review your partner contracts and the data you are sharing/receiving**

In recent enforcement actions, the Commission has made clear that a company's failure to employ "reasonable measures to safeguard health information it collected from consumers" constitutes an unfair business practice.⁷⁰ Specifically, in its case against BetterHelp, the Commission highlighted the company's failure "to contractually limit third parties from using Visitors' and Users' health information for their own purposes, including but not limited to research and improvement of their own products, when Respondent did not provide Visitors and Users notice or obtain their consent for such uses."⁷¹ What is more, the Commission has said companies that claim publicly to implement contractual protections limiting third party use, but instead fall back on mere "stock" contract language may be committing deceptive acts.⁷²

In light of the Commission's emphasis here, those that collect, share or receive potentially sensitive health information should prioritize steps to ensure partner contracts do not permit "unauthorized receipt, use, or onward disclosure of sensitive information" without first obtaining proper permissions.⁷³ Additionally, companies need also be cognizant of state-level contract requirements that may overlap in this area, particularly with respect to limiting processing of information to that which is "reasonably necessary."⁷⁴

Ultimately, companies should review their contracts, and make amendments where needed in order to avoid potential liability – even those that are only on the receiving end of the information. In situations where sensitive data is being shared among third parties, those involved should ensure that this sharing and processing is properly disclosed to consumers, that the information is properly permissioned, and that both state and federal contract requirements are in place.

- **Use benchmarking to establish a state law approach**

By the end of 2023, comprehensive privacy laws in California, Colorado, Connecticut, Utah, and Virginia will be effective, and many more will follow in subsequent years. For members of the digital advertising industry, this means coming into compliance

70. [In the Matter of, BetterHelp, Inc.](#), Complaint at 2 (March 2, 2023).

71. *Id.* at 15.

72. [U.S. v. GoodRx Holdings, Inc.](#), Complaint at 22 (Feb. 1, 2023).

73. Fed. Trade Comm'n, [Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases](#) (July 25, 2023).

74. See Colo. Rev. Stat. § 6-1-1305(5)(a).

with a patchwork of new obligations, many of which have not yet been interpreted by regulators. In the midst of this uncertainty, understanding the practices of other similarly situated companies – particularly with respect to sensitive information and inferences – may be beneficial for organizations seeking to better understand their potential liability in the absence of guidance. The NAI and our various working groups provide a trusted space for member companies and working group participants to accomplish this by comparing their practices to the broader industry and determining their course of action in accordance with their own risk tolerance and business judgment.

- ***Don't let perfect be the enemy of good***

As noted throughout this resource, the legal conclusions governing the use of sensitive health data are currently opaque, and are likely to remain that way for some time. As such, interpretations as to the kinds of business practices that are permissible will continue to evolve. Regulators have indicated that to some extent, they understand there is a necessary learning curve associated with novel legal requirements, and that coming into “perfect” compliance will take time and educational efforts.⁷⁵ Until the day a clear and comprehensive framework emerges for regulating non-HIPAA covered sensitive personal information, some of the most important steps companies can take now are to thoroughly evaluate their own data collection and handling practices, work to understand the different technologies they are using and where they are using them, revise data sharing contracts in accordance with state and federal requirements, and seek partnerships with other companies making good faith efforts to comply with relevant laws and practicing good data stewardship.

75. See [Attorney General Phil Weiser Launches Enforcement of Colorado Privacy Act](#) (July 12, 2023) (“As I’ve said publicly throughout the process, this Department’s enforcement of the Colorado Privacy Act is a critical tool to protect consumers’ data and privacy. Our enforcement of this important law will not seek to make life challenging for organizations that are complying with the law, but rather will seek to support such efforts,” said Weiser. “These letters will help make businesses aware of the law and direct them to educational resources to help them comply. And, if we become aware of organizations that are flouting the law or refusing to comply with it, we are prepared to act.”).

IV. Appendix

A. Defining “Sensitive Health” Information Across the U.S. Legal Regimes:

Federal		State Comprehensive	State Health Specific
Law/Regulation		Relevant Definition of “Health” Information	Obligation?
Federal	FTC (Section 5)	Information that is linked or reasonably linkable to an individual or device, and reveals a sensitive attribute about a consumer’s health status or history, including information that “could be linked to (or used to infer information about) chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, or sexual orientation.” ⁷⁶	Affirmative express consent required to collect, use or share/disclose. ⁷⁷

76. *U.S. v. GoodRx Holdings, Inc.*, Complaint at 4 (Feb. 1, 2023).

77. FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* at 47 (Feb. 2009).

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
Federal	FTC (HBNR)	<p>PHR identifiable health information means “individually identifiable health information,” as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information:</p> <p>(1) That is provided by or on behalf of the individual; and</p> <p>(2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.⁷⁸</p>	<p>“Consumer authorization” required before PHR Identifiable Information that is part of a personal health record can be shared. Without authorization, a “breach of security” has occurred and the entity must make required disclosures.⁷⁹</p>
	HIPAA Privacy Rule	<p>Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:</p> <p>(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and</p> <p>(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</p>	<p>Covered entities must obtain “authorization” before sharing PHI for marketing purposes.⁸⁰</p> <p>However, Business Associates can use/ disclose protected health information as permitted by agreement with covered entity.⁸¹</p>

78. 16 C.F.R. § 318.2(e).

79. 16 C.F.R. § 318.3.

80. 45 CFR § 164.508(a)(3).

81. U.S. Dep’t of Health and Human Serv., [Business Associate Contracts](#) (Jan. 25, 2013).

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
	HIPAA Privacy Rule	<p>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.⁸²</p> <p>Protected health information means individually identifiable health information:</p> <p>(1) Except as provided in paragraph (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.⁸³</p>	
State Comprehensive	California	Sensitive Personal information includes personal information “collected and analyzed concerning a consumer’s health.” ⁸⁴	Opt-out – If a covered business processes sensitive personal information for reasons other than those permissible under the statute, ⁸⁵ the business

82. 45 CFR § 160.103.

83. *Id.*

84. [California Consumer Privacy Act](#), Cal. Civ. Code §1798.140 (ae)(2)(B).

85. *Id.* at § 1798.121(a) (“use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185.”).

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
State Comprehensive	California		<p>must provide a link titled “Limit the use of my personal information” which functions as an opt out.</p> <p>Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this requirement.⁸⁶</p>
	Colorado	<p>Sensitive Data includes personal data “revealing a mental or physical health condition or diagnosis.”⁸⁷</p> <p>Sensitive data inference means “inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual’s racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.”⁸⁸</p>	Opt-in – Controllers must obtain consent to process sensitive data, including sensitive data inferences. ⁸⁹

86. *Id.* at § 1798.121(d).

87. [Colorado Privacy Act](#), Colo. Rev. Stat § 6-1-1303(24)(a).

88. 4 Colo. Code Regs. § 904-3-2.02.

89. 4 Colo. Code Regs. § 904-3-6.10.

Law/Regulation	Relevant Definition of “Health” Information	Obligation?
Connecticut	<p>Sensitive data includes personal data “revealing a mental or physical health condition or diagnosis”⁹⁰ or “consumer health data.”⁹¹</p> <p>Consumer Health Data means “any personal data that a controller uses to identify a consumer’s physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.”⁹²</p>	<p>Opt-in – Controller may not process sensitive data concerning a consumer without obtaining the consumer’s consent.⁹³</p> <p>Amendment adds further restrictions regarding the use and sale of consumer health data.⁹⁴</p>
Delaware	<p>Sensitive data includes personal data “revealing mental or physical health condition or diagnosis (including pregnancy).”⁹⁵</p>	<p>Opt-in – A controller shall not process sensitive data concerning a consumer without obtaining the consumer’s consent.⁹⁶</p>
Indiana	<p>Sensitive data includes personal data “revealing a mental or physical health diagnosis made by a health care provider.”⁹⁷</p>	<p>Opt-in – A controller shall not process sensitive data concerning a consumer without obtaining the consumer’s consent.⁹⁸</p>

90. [Connecticut Data Privacy Act](#), Conn. Gen. Stat. § 42-515(27).

91. CT Pub. Act No. 23-56 § 1(38) (“consumer health data” added to statutory definition through amendment in 2023).

92. CT Pub. Act No. 23-56 § 1(38) (definition of “consumer health data” added to statute through amendment in 2023).

93. [Connecticut Data Privacy Act](#), Conn. Gen. Stat. § 6(a)(4).

94. CT Pub. Act No. 23-56 § 2.

95. [Delaware Personal Data Privacy Act](#), 6 Del. C. § 12D-102(30)(a).

96. *Id.* at § 106(a)(4).

97. [Indiana Data Protection Act](#), IC. § 24-15-2-28.

98. *Id.* at § 24-15-4-1(5).

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
	Iowa	Sensitive personal data includes a “mental or physical health diagnosis.” ⁹⁹	Opt-out – A controller shall not process sensitive data collected from a consumer for a nonexempt purpose without the consumer having been presented with clear notice and an opportunity to opt out of such processing. ¹⁰⁰
	Montana	Sensitive data includes “data revealing mental or physical health condition or diagnosis.” ¹⁰¹	Opt-in – A controller may not process sensitive data concerning a consumer without obtaining the consumer’s consent. ¹⁰²
	Oregon	Sensitive data includes personal data that “reveals a consumer’s mental or physical condition or diagnosis.” ¹⁰³	Opt-in – A controller may not process sensitive data about a consumer without first obtaining the consumer’s consent. ¹⁰⁴

99. [Iowa Consumer Data Protection Act](#), Iowa Code § 715D.1(26).

100. *Id.* at § 715D.4(2).

101. [Montana Consumer Data Privacy Act](#), S.B. 0384 § 2(24)(a).

102. *Id.* § 7(2)(b).

103. [Oregon Consumer Privacy Act](#), S.B. 619 §1(18)(A).

104. *Id.* at §5(2)(b).

Law/Regulation	State	Relevant Definition of “Health” Information	Obligation?
	Tennessee	Sensitive data includes personal information “revealing mental or physical health diagnosis.” ¹⁰⁵	Opt-in – A controller may not process sensitive data concerning a consumer without obtaining the consumer’s consent. ¹⁰⁶
	Texas	Sensitive data includes personal data “revealing mental or physical health diagnosis.” ¹⁰⁷	Opt-in – A controller may not process the sensitive data of a consumer without obtaining the consumer’s consent ¹⁰⁸
	Utah	Sensitive data includes 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.” ¹⁰⁹	Opt-out – Must present consumers with clear notice and an opportunity to opt-out before processing sensitive information. ¹¹⁰
	Virginia	Sensitive personal data includes data revealing “a mental or physical health diagnosis.” ¹¹¹	Opt-in – Controller shall not process sensitive data without obtaining consumer consent. ¹¹²

105. [Tennessee Information Protection Act](#), Tenn. Code Ann. § 47-18-3201(25).

106. *Id.* at § 47-18-3204(a)(6).

107. [Texas Data Privacy and Security Act](#), H.B. 4 §541.001(29).

108. *Id.* at §541.101(b)(4).

109. [Utah Consumer Privacy Act](#), Utah Code Ann. § 13-61-101(32).

110. *Id.* at § 13-61-302(3).

111. [Virginia Consumer Data Protection Act](#), Va. Code Ann. § 59.1-575.

112. *Id.* at § 59.1-578(A)(5).

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
State Health Specific	Washington	<p>“Consumer health data” means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status.</p> <p>For the purposes of this definition, physical or mental health status includes, but is not limited to:</p> <ul style="list-style-type: none"> (i) Individual health conditions, treatment, diseases, or Diagnosis; (ii) Social, psychological, behavioral, and medical Interventions; (iii) Health-related surgeries or procedures; (iv) Use or purchase of prescribed medication; (v) Bodily functions, vital signs, symptoms, or measurements of the information described in this definition; (vi) Diagnoses or diagnostic testing, treatment, or medication; (vii) Gender-affirming care information; (viii) Reproductive or sexual health information; (ix) Biometric data; (x) Genetic data; (xi) Precise location information that could reasonably indicate a consumer’s attempt to acquire or receive health services or Supplies; (xii) Data that identifies a consumer seeking health care services; or 	Separate and distinct consumer consent required before collection or sharing, and signed “valid authorization” required before sale. ¹¹³

113. [“My Health, My Data” Act \(MHMD\)](#), H.B. 1155 § 5(1)(a)-(b), § 9(1).

Law/Regulation	Relevant Definition of “Health” Information	Obligation?
State Health Specific	<p>Washington</p> <p>(xiii) Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in this definition that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).¹¹⁴</p>	
	<p>Nevada</p> <p>“Consumer health data” means 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.</p> <p>The term: Includes, without limitation:</p> <p>Information relating to: (1) Any health condition or status, disease or diagnosis; (2) Social, psychological, behavioral or medical interventions; (3) Surgeries or other health-related procedures; (4) The use or acquisition of medication; (5) Bodily functions, vital signs or symptoms; (6) Reproductive or sexual health care; and (7) Gender-affirming care;</p> <p>Biometric data or genetic data related to information described in this definition;</p>	<p>Separate and distinct consumer consent required before collection or sharing, and signed “valid authorization” required before sale.¹¹⁵</p>

114. *Id.* at § 3(8).

115. [Nevada](#) S.B. 370 §22, §30.

Law/Regulation		Relevant Definition of “Health” Information	Obligation?
	Nevada	<p>Information related to the precise geolocation information of a consumer that a regulated entity uses to indicate an attempt by a consumer to receive health care services or products; and</p> <p>Any information described in this definition that is derived or extrapolated from information that is not consumer health data, including, without limitation, proxy, derivative, inferred or emergent data derived through an algorithm, machine learning or any other means. Does not include information that is used to: Provide access to or enable gameplay by a person on a video game platform; or Identify the shopping habits or interests of a consumer, if that information is not used to identify the specific past, present or future health status of the consumer.¹¹⁶</p>	

116. NV S.B. 370 § 8.

B. Requirements for Obtaining Consent Across the U.S. Legal Regimes

Federal		State Comprehensive	State Health Specific
Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information	
Federal	FTC (Sec. 5)	<p>“Affirmative Express Consent” means any freely given, specific, informed, and unambiguous indication of an individual consumer’s wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of:</p> <ol style="list-style-type: none"> 1) the categories of information that will be collected; 2) the specific purpose(s) for which the information is being collected, used, or disclosed; 3) the names or categories of Third Parties (e.g., “analytics partners” or “advertising partners”) collecting the information, or to whom the information is disclosed, provided that if Respondent discloses the categories of Third Parties, the disclosure shall include a hyperlink to a separate page listing the names of the Third Parties; 4) a simple, easily located means by which the consumer can withdraw consent; and 5) any limitations on the consumer’s ability to withdraw consent.¹¹⁷ 	
	FTC (HBNR)	<p>The text of the HBNR does not define the “consumer authorization” required to share PHR Identifiable Health Information in a Personal Health Record. However, the Commentary to the original rule suggests situations that constitute “unauthorized used.”¹¹⁸</p>	

117. *In the Matter of, BetterHelp, Inc.*, Decision and Order at 2 (March 2, 2023).

118. NPRM at 37824, N49 (“[d]ata sharing to enhance consumers’ experience with a PHR is authorized only ‘as long as such use is consistent with the entity’s disclosures and individuals’ reasonable expectations’ and that ‘[b]eyond such uses, the Commission expects that vendors of personal health records and PHR related entities would limit the sharing of consumers’ information, unless the consumers exercise meaningful choice in consenting to such sharing. Buried disclosures in lengthy privacy policies do not satisfy the standard of ‘meaningful choice.’” (74 FR 42967).

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
Federal	HIPAA Privacy Rule	<p>“Authorization” to disclose PHI for marketing purposes requires</p> <ol style="list-style-type: none"> 1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion; 2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure; 3) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure; 4) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose; 5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository; 6) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual must also be provided.¹¹⁹

119. 45 CFR § 164.508(c).

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
State Comprehensive	California	Businesses that use or disclose a consumer's sensitive personal information for purposes other than those authorized by the statute must 1) provide a clear and conspicuous "Do not sell my personal information" link on homepage that enables an opt-out of the sale or sharing of personal information; 2) provide a clear and conspicuous "Limit the use of my sensitive personal information" link on homepage. ¹²⁰
	Colorado	Consent to process sensitive personal information means clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data. Consent does not include: Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, Hovering over, muting, pausing, or closing a given piece of content, and Agreement obtained through dark patterns. ¹²¹
	Connecticut	Consent to process sensitive personal information means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. Consent may include a written statement, including by electronic means, or any other unambiguous affirmative action.

120. [California Consumer Privacy Act](#), Cal. Civ. Code § 1798.135.

121. [Colorado Privacy Act](#), Colo. Rev. Stat § 6-1-1303(5).

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
State Comprehensive	Connecticut	Consent does not include acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, hovering over, muting, pausing or closing a given piece of content, or agreement obtained through the use of dark patterns. ¹²²
	Delaware	<p>Consent to process sensitive personal information means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. Consent may include a written statement, including by electronic means, or any other unambiguous affirmative action.</p> <p>Consent does not include any of the following:</p> <ul style="list-style-type: none"> a. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information. b. Hovering over, muting, pausing, or closing a given piece of content. c. Agreement obtained through the use of dark patterns.¹²³
	Indiana	Consent to process sensitive personal information means a clear affirmative act that signifies a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. For purposes of this section, a clear affirmative act includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. ¹²⁴

122. [Connecticut Data Privacy Act](#), Conn. Gen. Stat. § 42-515(6).

123. [Delaware Personal Data Privacy Act](#), 6 Del. C. § 12D-102(7).

124. [Indiana Data Protection Act](#), IC. § 24-15-2-7(a).

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
	Iowa	“Clear notice and opportunity to opt-out of processing” of sensitive personal information is not defined by the statute.
	Montana	<p>Consent to process sensitive personal information means a clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. The term may include a written statement, a statement by electronic means, or any other unambiguous affirmative action.</p> <p>The term does not include: (i) acceptance of a general or broad term of use or similar document that contains descriptions of personal data processing along with other unrelated information; (ii) hovering over, muting, pausing, or closing a given piece of content; or (iii) an agreement obtained using dark patterns.¹²⁵</p>
	Oregon	Consent to process sensitive personal information means an affirmative act by means of which a consumer clearly and conspicuously communicates the consumer’s freely given, specific, informed and unambiguous assent to another person’s act or practice under the following conditions: The user interface by means of which the consumer performs the act does not have any mechanism that has the purpose or substantial effect of obtaining consent by obscuring, subverting or impairing the consumer’s autonomy, decision-making or choice; and The consumer’s inaction does not constitute consent. ¹²⁶

125. [Montana Consumer Data Privacy Act](#), S.B. 0384 § 2(5).

126. [Oregon Consumer Privacy Act](#), S.B. 619 § 1(6).

Law/Regulation	Definition of consent/Notice Requirements before processing of sensitive health information
Tennessee	Consent to process sensitive personal information Means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer; and Includes a written statement, including a statement written by electronic means, or an unambiguous affirmative action. ¹²⁷
Texas	Consent to process sensitive personal information means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. The term does not Include: acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; hovering over, muting, pausing, or closing a given piece of content; or agreement obtained through the use of dark patterns. ¹²⁸
Utah	Clear and conspicuous notice of the collection the right to opt-out of the processing of sensitive personal information is not defined by the statute.
Virginia	Consent to process sensitive personal information requires a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. ¹²⁹

127. [Tennessee Information Protection Act](#), Tenn. Code Ann. § 47-18-3201(6).

128. [Texas Data Privacy and Security Act](#), H.B. 4 § 541.001(6).

129. [Virginia Consumer Data Protection Act](#), Va. Code Ann. § 59.1-575.

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
State Health Specific	Washington	<p>To collect or share consumer health data, covered businesses must obtain consumer consent, except for instances allowed by the statute. Consents must be separate and distinct. Consent means a clear affirmative act that signifies a consumer’s freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means.</p> <p>Consent may not be obtained by: A consumer’s acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information; A consumer hovering over, muting, pausing, or closing a given piece of content; or A consumer’s agreement obtained through the use of deceptive designs.¹³⁰</p> <p>To sell consumer health data, covered businesses must obtain consumer authorization, which includes (a) The specific consumer health data concerning the consumer that the person intends to sell; (b) The name and contact information of the person collecting and selling the consumer health data; (c) The name and contact information of the person purchasing the consumer health data from the seller identified in (b) of this Subsection; (d) A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser identified in (c) of this subsection when sold; (e) A statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization; (f) A statement that the consumer has a right to revoke the valid authorization at any time and a description on how to submit a revocation of the valid authorization;</p>

130. [“My Health, My Data” Act \(MHMD\)](#), H.B. 1155 § 3(6).

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
State Health Specific	Washington	(g) A statement that the consumer health data sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by this section; (h) An expiration date for the valid authorization that expires one year from when the consumer signs the valid authorization; and (i) The signature of the consumer and date. ¹³¹
	Nevada	To collect or share consumer health data, a covered business must obtain separate and distinct instances of affirmative, voluntary consent, except where allowed by the statute. ¹³² To sell consumer health data, a covered business must obtain written authorization of the consumer, which includes (a) The name and contact information of the person selling the consumer health data; (b) A description of the specific consumer health data that the person intends to sell; (c) The name and contact information of the person purchasing the consumer health data; (d) A description of the purpose of the sale, including, without limitation, the manner in which the consumer health data will be gathered and the manner in which the person described in paragraph (c) intends to use the consumer health data; (e) A statement of the provisions of subsection 2; (f) A statement that the consumer may revoke the written authorization at any time and a description of the means established pursuant to subsection 4 for revoking the Authorization; (g) A statement that any consumer health data sold pursuant to the written authorization may be disclosed to additional persons and entities by the person described in paragraph (c) and, after such disclosure, is no longer subject to the protections of this section;

131. *Id.* at § 9(2).

132. [Nevada](#) S.B. 370 § 22.

Law/Regulation		Definition of consent/Notice Requirements before processing of sensitive health information
	Nevada	(h) The date on which the written authorization expires pursuant to subsection 5; and (i) The signature of the consumer to which the consumer health data pertains. ¹³³

C. Other obligations to keep in mind when processing sensitive health information

- 1. FTC Section 5 Partner Contract Requirements:** When sharing health information, companies must contractually limit if and how third parties can use that information, and accurately disclose this in their privacy policy/public facing disclosures.¹³⁴
- 2. State DPA/DPIA requirements:** When a business processes sensitive information, most state comprehensive privacy laws require that it make available upon request, a report weighing the benefits and harms of the processing, along with the mitigating factors taken to prevent such harm.
- 3. Privacy policy requirements:** most State privacy laws, as well as Section 5 of the FTC Act require businesses that collect or process sensitive information to disclose such activity in its consumer facing privacy policy. State laws generally require the categories of sensitive information processes to be disclosed, while the FTC has said it expects businesses processing sensitive information to disclose the sensitive information they process, and how they use it or risk facing a deception charge.

D. HHS Privacy Rule Business Associate Agreement Requirements

In order to share PHI without running afoul of the Privacy Rule, covered entities must enter a contractual agreement with business associates known as a “business associate agreement” – the agreement must:

1. Establish permitted and required uses/ disclosures of PHI,
2. Limit the business associate’s use of the PHI other than as permitted by the contract or required by law,

133. *Id.* at § 30(3).

134. [In the Matter of, BetterHelp, Inc.](#), Agreement Containing Consent Order at 2 (Mar. 2023).

3. Require the business associate to implement appropriate safeguards to prevent unauthorized use/disclosure,
4. Require the business associate to report any use/disclosure outside of the contract to the covered entity,
5. Require the business associate to disclose PHI to satisfy the covered entity's obligation based on consumer access requests,
6. To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation,
7. Require business associate to make certain internal practices available to the HHS to ensure the covered entities compliance with the rule,
8. Require the business associate to return or destroy (to the extent feasible) all PHI created/received by business associate on behalf of covered entity at the end of the relationship,
9. Require business associates to hold subcontractors with access to the PHI to the same standards the business associate itself is bound to through this contract, and
10. Authorize termination of contract by covered entities should the business associate materially violate the agreement.¹³⁵

135. U.S. Dep't of Health and Human Serv., [Business Associate Contracts](#) (Jan. 25, 2013).