September 28, 2023

The Honorable Bill Cassidy
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate
Washington, DC 20510

Dear Senator Cassidy,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to comment in response to the Request for Information from Stakeholders on Improving Americans' Health Data Privacy ("RFI"). Please see below detailed responses to the thoughtful questions you raised in the RFI. In summary, the NAI makes the following key recommendations on this important subject:

- Congress should promote the critical role of data-driven health advertising, which is extremely valuable to consumers and health care professionals ("HCPs"). Consumers benefit by being connected with medical treatments, medications, or information they genuinely need or want, as well receiving coupons and discounts for medications. HCPs benefit because data-driven health advertising improves the viability of clinical trials and helps improve health equity for individuals with limited access to health information and treatment.
- Congress should enact a comprehensive consumer privacy law, which will create a uniform national framework to protect consumers' personal information, rather than expanding the scope of HIPAA to cover a broader range of health data. This approach is the best way to provide greater protections for all Americans and can protect health information not currently covered by HIPAA. Such a framework should focus on preventing harmful outcomes, rather than creating broad limitations on access or uses of health information.
- A national privacy law should clearly define sensitive health information and distinguish its use from that of non-sensitive information, while focusing on *uses* of this information, regardless of sensitivity, because all consumer information can be used for either beneficial or harmful purposes.

Additionally, please find attached with these comments a recent legal and regulatory analysis produced by NAI that catalogs the various state and federal approaches to defining sensitive health information and explains the way various legal interpretations impact the digital advertising industry. This analysis also summarizes recent federal enforcement actions and proposed regulatory updates pertaining to sensitive health data by the Federal Trade Commission ("FTC" or "Commission") and poses a set of recommendations for companies to protect consumer health data and comply with the various U.S. state and federal laws.

I. About the NAI

Founded in 2000, the NAI is the leading non-profit, self-regulatory and trade association for advertising technology companies. For over 20 years the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest industry standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust. As a non-profit organization, the NAI promotes the health of the digital media ecosystem by maintaining strong privacy standards for the collection and use of data for digital advertising across all digital media. The NAI Code of Conduct (the "NAI Code") has long promoted strong self-regulatory standards for its members and required its members to undergo annual privacy accountability reviews by NAI staff attorneys.[1]

II. Introduction and the Benefits of Data-Driven Health Advertising

Data-driven health advertising is an extremely valuable tool that helps connect consumers and HCPs with medical treatments, medications, or information they genuinely need or want, as well as coupons and discounts for medications. Data-driven health advertising helps consumers by connecting them with health information that is more relevant to them, therefore helping to improve health equity for individuals with limited access to health information and treatment. In short, data-driven advertising is a critical source of information that empowers individual citizens to control their own health. For example, health-related advertising can drive early awareness of health conditions and treatments – and the earlier a person is made aware of a relevant condition or treatment, the greater their opportunity to secure a positive health outcome. Health-related advertising also improves the viability of clinical trials and other messaging related to rare conditions falling under the Orphan Drug Act[2] which incentivizes the development of treatments and medications for conditions affecting fewer than 200,000 people in the United States, including Huntington's disease, myoclonus, ALS, Tourette syndrome, and muscular dystrophy.

The FTC recently cited the important role that advertising directed to HCPs plays in drug prices by making HCPs aware of potentially lower-cost alternative treatments.[3] Specifically, the Commission stated that, "[h]ealthcare digital advertising is a nearly $14 billion industry that is expected to continue growing, due in part to increasing demand for digital advertising. While still emerging, the market for HCP programmatic advertising—a subset of the total healthcare digital advertising industry—has grown significantly in recent years, accelerated by the COVID-19 pandemic, which caused healthcare companies to shift sales activities away from traditional in-office physician detailing and toward online marketing." The Commission went on to assert that reduced competition in HCP programmatic advertising would result in "increased prices, reduced choice, and diminished innovation."[4]

---

[1] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[2] Orphan Drug Act, Pub. L. No. 97-414, 96 Stat. 2049.

[3] Compl. at 2, *In re IQVIA Holdings, Inc.*, FTC File No. 2210196 (July 17, 2023).

[4] *Id.* at 2-3.

Of course, it is also essential that benefits of health-related advertising are achieved in a manner that protects consumer privacy. This objective is at the core of the NAI's mission as the leading privacy self-regulatory association for the advertising technology industry. The NAI has promoted the highest voluntary industry standards around the use of sensitive data, including sensitive health data. As a result, NAI members play an important role in educating consumers about various medications and treatments that may be relevant to them, and by providing them resources to actively participate in their own healthcare, all while adhering to strong privacy practices. These comments draw from the NAI's leadership in this area, highlighting key elements for public policies to successfully strike a balance between privacy protections, while retaining the substantial benefits of data-driven health advertising.

III. General Questions & Applicability of HIPAA

In this section, we address a series of general questions raised in the RFI regarding the different types of consumer health information, and how they are similar or dissimilar. We also address multiple questions pertaining to the Health Insurance Portability and Accountability Act ("HIPAA"). NAI members generally are not covered entities for purposes of HIPAA applicability, and generally do not handle protected health information regulated by HIPAA, unless acting in the capacity of a business associate or a service provider. Therefore, the NAI will not comment specifically on the effectiveness of HIPAA for regulating covered entities.

However, consumer "health information" is now understood to include more than just prescription records, medical diagnoses issued by doctors, or other traditionally HIPAA-covered data. This is shown by the definitions of "sensitive data" seen in some recently passed state privacy laws and recent enforcement actions initiated by the FTC. But even before being required to do so by certain new state laws, NAI members committed to obtaining opt-in consent prior to collecting or using *sensitive* health information for Tailored Advertising or Ad Delivery and Reporting purposes.[5] This includes information other than HIPAA-covered health information, such as information related to a sensitive health condition that a consumer enters manually into a website or app that is not a HIPAA-covered entity. Further, the NAI Code also acknowledges that browsing or purchase history related to a consumer's sensitive health condition constitutes sensitive information.

The NAI recognizes the nuance associated with the processing of non-HIPAA health information, and the corresponding need for a definition of "sensitive health information" that warrants a higher level of privacy protection. This definition should properly strike the balance between being overly specific in a way that misses important categories of sensitive health information, or excessively broad in a way that makes the categories that deserve enhanced protections meaningless. For this reason, the NAI's traditional approach to health information has been to differentiate between *sensitive* health conditions, such as cancers and STDs, and *non-sensitive* health conditions, such as seasonal allergies and the common cold.

However, several new state laws have recently taken a starkly different approach to defining non-HIPAA sensitive health information, opting for overly-broad definitions that threaten to sweep large amounts of non-sensitive information into a category accompanied by use limitations, heightened notice and consent requirements, and other onerous requirements that

[5] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter "NAI Code"] § II.C.1.e, https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

limit the utility of information that is not sensitive without any corresponding privacy benefit to consumers.[6] Indeed, the overbreadth of these definitions threaten serious negative implications—stifling competition and growth, and degrading the consumer's online experience. For example, some definitions of "sensitive" health information are so broad that they could cover the fact that a consumer purchased running shoes, which might reveal an overall interest in health and fitness. Further, while the NAI does consider inferences about sensitive health or medical conditions to be sensitive health data, many of the state laws and regulations are ambiguous regarding what constitutes an inference, applying merely to information that "may reveal" a sensitive health condition.[7]

Such overly broad definitions of health information diminish the significance of the sensitive classification more broadly. If all data that is even remotely health-related is considered sensitive, such as information about browsing for multivitamins or purchasing running shoes,[8] the significance of safeguarding highly sensitive information such as that which reveals a consumer's cancer diagnosis would be diminished. It is essential that public policies addressing consumer health information strike the right balance, rather than broadly prohibiting myriad valuable uses of consumer information, including but not limited to data-driven health advertising.

HIPAA's current scope is clear and effective. It is focused on the privileged relationship between patients and providers of healthcare, and the data shared among them (for and on behalf of patients, including with insurers and other service providers). In this way, HIPAA appropriately ensures that patients are not forced to make decisions about their healthcare based on how providers and insurers use patient data.

With respect to the scope and dual goals of HIPAA–to improve the portability of health records and increase the number of Americans with health insurance–we strongly discourage Congress from attempting to expand it to include consumers' health-related information collected from sources other than HIPAA-covered entities.[9] The public policy interests in protecting patient healthcare information reflected by HIPAA do not align with the interests in protecting consumer information collected in other contexts, which –while still important – should be separately regulated from patient data under HIPAA.

Over the course of the last 12 months, the FTC has asserted its authority to regulate non-HIPAA health information using the Health Breach Notification Rule ("HBNR") and Section 5 of the FTC Act, specifically as demonstrated by enforcement actions against GoodRx, BetterHelp and other

---

[6] *See, e.g.* Wash. Rev. Code § 19.373.010(8)(a) (defining consumer health data); Wash. Rev. Code § 19.373.010(8)(b)(xiii) (providing that consumer health data includes "[a]ny information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data… derived or extrapolated from non-health information"); Colo. Rev. Stat. § 6-1-1303(24)(a) (2023) (defining sensitive data as personal data "revealing… a mental or physical health condition or diagnosis").

[7] For example, California regulations restricting the use and collection of personal data direct businesses to consider "possible negative impacts on consumers posed" by the collection and processing of personal data. In an example provided in the regulations, the collection of precise geolocation "may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers," and that this is a "possible negative impact[ ]" a business must consider. *See* Cal. Code Regs. tit. 11 § 7002(d)(2).

[8] Wash. Rev. Code § 19.373.010(8) (defining consumer health data). Wash. Rev. Code § 19.373.010(8)(b)(xiii) (describing information derived or extrapolated from non-health data).

[9] Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research (Sharyl J. Nass et al. eds., 2009),https://www.ncbi.nlm.nih.gov/books/NBK9576/#:~:text=The%20Health%20Insurance%20Portability%20and,Americans%20with%20health%20insurance%20coverage.

consumer-facing companies,[10] and its parallel effort to update the HBNR.[11] However, the Commission's expectations and the scope of health information under its authority remain unclear. While the NAI largely agrees with the objectives of the Commission to clarify the application of the HBNR, it is faced with a daunting challenge of adapting new regulations and enforcement of modern practices around a law that was crafted more than a decade ago with the primary goal of ensuring consumer notice to malicious breaches of their medical records.

The NAI therefore urges Congress to pass a comprehensive national privacy law that would help to clarify the application of existing laws and regulations, such as the application of the FTC's authority under Section 5 of the FTC Act, prohibit unreasonable and harmful practices associated with consumers personal information–both sensitive and non-sensitive– and create a singular national privacy framework that replaces the current state patchwork of laws that have been enacted over the last several years.

With respect to a duty of loyalty as it might be applied under HIPAA or to processors of sensitive health data more broadly, the greatest challenge would be to clearly define what these novel duties would require of companies. For example, many proposed duties of loyalty would require businesses to consider when it is reasonably foreseeable that a process will be against a consumer's physical, financial, psychological, or reputational interests and notify the consumer about that potential harm. Such a requirement would obligate each covered entity to independently assess when data processing would be against a particular consumer's psychological or reputational interests. Such considerations are extremely individualized and subjective, and each business (and each consumer) may reach a different conclusion. The lack of clarity on this point is likely to create unnecessary risk for businesses and foster unclear expectations for consumers.

IV. Collecting Health Data

Since its inception in 2000, the NAI has championed consumer choice and transparency among its members regarding consumers' personal information collected for advertising and marketing. As noted above, the NAI has long advocated that before information revealing an individual's sensitive health condition is collected or used for targeted advertising, a user must "manifest the intent to opt in to an activity described in a clear and conspicuous notice."[12] Meaningful notice should clearly explain the proposed uses of the information upon collection and the users rights associated with it, and avoid deceptive design tactics that could trick users into making choices they don't necessarily intend or fully understand. In 2022, the NAI released a thorough set of *Best Practices for User Choice and Transparency*, which detailed specific recommendations to encourage companies to maximize transparency and choice for consumers around the collection and use of their data for advertising and marketing purposes, specifically seeking to prevent data collection practices sometimes referred to as "dark patterns," because they have the effect of misleading consumers and preventing informed decision making.[13]

---

[10] Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, FTC (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

[11] Health Breach Notification Rule, 88 Fed. Reg. 37,819 (proposed June 9, 2023).

[12] NAI Code §I.H.

[13] *NAI Best Practices for User Choice and Transparency*, Network Advert. Initiative (2022), https://thenai.org/wp-content/uploads/2022/05/NAI-Dark-Patterns-Final-5.12.22.pdf.

Nearly every comprehensive privacy law in the United States and abroad contemplates the notion that personal data exists on a spectrum of sensitivity, with certain types of data requiring a higher level of legal protection. However, excessively broad definitions of sensitive health information, particularly in states like Washington and Nevada, could be interpreted to include nearly all remotely health-related personal information. This is particularly true with the Washington My Health My Data Act, which contains a private right of action, and therefore is highly concerning because it subjects companies of all sizes to engage in costly litigation to defend against lawsuits brought around the law's broad, ambiguous definition of consumer health data.

Short of halting the function of the internet completely, widespread adoption of these unreasonable definitions could result in consumer consent being required for routine collection and processing of virtually all consumer information. Not only would this be cumbersome and time consuming for the user, but it would also render the intended efficacy of the notice obsolete. If confronted with opt-in notices dozens of times daily, consumers are likely to develop "consent fatigue," skipping through privacy notices altogether and accepting to simply use the internet efficiently, without properly distinguishing between more sensitive types of data or processing activities. There is a wide range of research that supports the notion that the consent process, and particularly the ability to enable consumers to make an informed choice about their data, is threatened by excessive use of "notice-and-choice." For instance, a recent European study that found 72% of 16-34 year olds were "annoyed" by the amount of times they were asked to provide consent on the internet.[14]

Therefore, an effective national privacy law should promote effective transparency and control mechanisms for consumers, without extending opt-in requirements too broadly, and should encourage the deployment of user interface guidelines such as those suggested by the NAI. However, while meaningful "notice and choice," practices provide an essential tool for consumers, these should not be the core focus of a national privacy law. It is widely recognized that the notice and choice approach can place an outsized burden on consumers and provide for limited protections, particularly when implemented too rigidly. Instead, a national privacy law should primarily focus on defining and preventing harmful uses of consumers' personal information and encourage transparency and control to enhance consumer understanding of benign data uses.

V. Location Data

There are a wide range of industry practices that rely on the collection and processing of Precise Location Information (PLI) that are beneficial to institutions that provide health services to citizens. For instance, this data is used to support both private businesses as well as municipalities in understanding foot traffic, supply chains, and commuting patterns in connection with the places of interest that make up the communities and neighborhoods we live in. This naturally includes hospitals and other medical facilities. As an example, most major infrastructure developments undergo years of pre-construction research where stakeholders leverage location data to ensure that a project is being built where it will best serve the interests of a given

[14] Michael Feeley, *Research Reveals What Online Value Exchange Means for Millennials and Gen Z*, The Drum (Oct. 5, 2018), https://www.thedrum.com/news/2018/10/05/research-reveals-what-online-value-exchange-means-millennials-and-gen-z.

community. This is especially true for hospitals, as limited community resources require that these multi-billion-dollar infrastructure projects are correctly placed in locations that will maximize their economic value and ensure social equity by providing equal access to medical care.

In an effort to address potential harms and retain the availability of the positive use cases associated with precise consumer geolocation information, the NAI developed a set of Voluntary Enhanced Standards for Precise Location Information Solution Providers ("Standards") in June 2022.[15] These Standards created restrictions on the use, sale, or transfer of precise location information associated with sensitive points of interest (POIs), including but not limited to sensitive medical facilities where consumers expect and deserve heightened standards of care. The goal of the NAI's Standards is to limit contextual information from being associated with POIs that an average person regards to be more sensitive in nature, thus preventing their clients, and other market participants downstream, from using such contextual information for any purpose. While the list of sensitive medical locations is extensive, we made a practical decision to include only those where a heightened sense of privacy would likely be desirable by the average person, therefore choosing to exclude medical facilities such as pharmacies, hospitals, general practitioner, and dental facilities, as well as potentially health-related facilities such as fitness clubs. In addition, the NAI has also been a leader in encouraging and educating companies about how they can render PLI imprecise.[16]

In contrast to the NAI Standards, four state laws enacted this year created broad, ambiguous restrictions on the use of consumers' precise location information related to healthcare facilities, defined broadly.[17] These laws do not make the same practical distinctions as the NAI standards. Instead, they adopt overly broad definitions of covered healthcare facilities that not only apply to pharmacies, hospitals, and general practitioner offices, but also possibly fitness clubs and other more general points of interest. These laws, depending on their interpretation and the application of the private right of action in the Washington health law, could disrupt important projects and initiatives that rely upon utilizing consumer location data around medical facilities.

The NAI encourages policymakers to consider these resources to develop a balanced approach to protecting consumer location information, rather than enacting broad bans on collection, use or sales of such information. Particularly our list of sensitive points of interest provides a pragmatic approach to identifying what might constitute a location where consumers deserve heightened protections regarding the processing or sharing of their precise location information.

---

[15] *See NAI Precise Location Information Solution Provider Voluntary Enhanced Standards*, Network Advert. Initiative (2022), https://thenai.org/wp-content/uploads/2022/06/Precise-Location-Information-Solution-ProviderVoluntary-Enhanced-Standards.pdf.

[16] *See Guidance for Members: Determining Whether Location is Imprecise*, Network Advert. Initiative (2020), https://thenai.org/wp-content/uploads/2021/07/nai_impreciselocation2-1.pdf.

[17] Andreas T. Kaltsounis & Nichole L. Sterling, *State Laws Limiting Geolocation Tech Around Health Centers Pose Compliance Challenges*, Law360 (https://admin.bakerlaw.com/wp-content/uploads/2023/08/Law360-4-New-State-Geofencing-Bans-And-How-They-Differ.pdf).

VI. Sharing Health Data, Financial Data, and the Need for Data Stewardship and Appropriate Safeguards

The RFI raises a series of important questions about the sharing of data covered under the HIPAA framework, including the appropriate approach to de-identification and safeguards for sharing and processing of this data, and the role, oversight and potential regulation of third parties. These are all very important questions, both with respect to the application of HIPAA and for the development of an effective national consumer privacy law that provides coverage for consumer health data more broadly.

The NAI supports HIPAA's clear and defined approach to de-identification, which enables HIPAA Covered Entities, Business Associates, researchers, and other third parties to leverage (de-identified) data to help advance the health and care industry, in a trusted way. This is a unique and valuable approach that does not exist more broadly in most other U.S. privacy laws. De-identification is widely recognized as effective for making consumer data not "reasonably linkable," and therefore not "personal information," but many state laws don't effectively define how this threshold can be met. This is a critical element in establishing clear business processes that can be relied upon by companies using this data, in the same way that industry standard audits (e.g., SOC II) can be relied upon to show the adequacy of other business practices. This approach should also be incorporated into a national consumer privacy law.

VII. Artificial Intelligence

The NAI has long promoted public policies pertaining to artificial intelligence and automated decision making that differentiate between decisions that produce legal effect and those that do not. For example, artificial intelligence can be used to extend an interview to a job applicant, based on a computer's reading of the applicant's resume, and an algorithm's ability to rank that resume against other applicants. However, decisions like these can carry legal effects–the algorithm may, for example, be biased in favor of white applicants compared to Black applicants or be biased in favor of men compared to women.

The use of a certain demographic, such as gender, is entirely different if used by automated decision-making tools to serve an advertisement than to make a hiring decision. The NAI has therefore consistently advocated for a harm-based approach to regulations around this type of technology; that is, AI's beneficial use cases must be balanced against the negative use cases. Processing that produces legal effects—*e.g.*, processing that affects an individual's rights, status, or rights under a contract—or similarly significantly affects a data subject is the kind of processing that should be considered the most sensitive, where greater oversight is practical and an opportunity for individuals to opt out would be most necessary.

Ultimately, a consumer's right to opt out of processing through AI, including profiling, should vary depending on certain factors. The benefits of AI in certain circumstances counsel against an overly broad right to opt out of all automated decision making. Therefore, laws and regulations should guide businesses to adopt a risk-based approach that focuses on outcomes from automated decision making that could have a harmful impact on consumers. When a consumer is served an advertisement based on an inferred interest in cross-country skiing, the harm to the consumer is small to nonexistent. Conversely, when a consumer is subjected to tailored advertising that pertains to eligibility determinations, there is a greater risk of harm or disparate impact. Many states now require companies to conduct mandatory Data Protection Assessments

("DPAs") that can play a key role in protecting consumers from adverse effects of AI. During this process, companies should consider the role AI plays in their business and the potential increased risk to consumers, ultimately determining where human oversight would be beneficial.

With respect to health data, algorithms and AI are increasingly essential for analyzing health data to maximize effective reach to consumers, such as to determine how most effectively to deliver information on treatments and care. It is essential to protect against harmful outcomes discussed above, particularly to prevent disparate outcomes, and to maximize diversity and inclusion. However, specific limitations regarding how and when health data should be used, or around the application of AI, can also induce biases in the data. This increases the risk of incorrect predictions and unforeseen errors in the development of health models, possibly causing an otherwise functional and beneficial approach to make poor predictions. Therefore, data protection assessments should be applied for handling of consumer health data, with a focus on the application of any analytical outputs, rather than the AI itself.

VIII. State and International Privacy Frameworks

As discussed previously in these comments and cited in the RFI, myriad states have recently enacted privacy laws, and U.S. businesses are faced with a growing patchwork of disparate state consumer privacy laws. In addition to the 12 broad consumer privacy laws enacted over the last several years, narrower legislation has been enacted or is actively being considered across nearly a dozen other states. This approach is neither in the best interest of consumers, nor businesses who are struggling to comply.

For many years, the NAI has been a leading industry proponent of a comprehensive national privacy framework to provide clear rules for *all* businesses operating in the United States, not just those volunteering to submit to such standards, as well as additional privacy enhancements for consumers, and it would replace the patchwork of state consumer privacy laws across the country. As discussed previously in these comments, such a framework should provide strong protections against unexpected and harmful outcomes of data processing and allow for innovative uses of data for advertising and the social good, rather than create broad bans on data collection and use, which is impractical and undesirable. Not only is strong preemption a critical element of an effective national framework, it should also provide for exemptions of data covered by existing law, such as HIPAA.

Of course, there are also many international laws and regulations in place regarding consumer data, that while similar in some respects, also diverge in other key areas. While the NAI encourages Congress to maximize interoperability with key international frameworks, we also believe that U.S. citizens would be well served by the unique approach we have described that places a greater emphasis on beneficial uses of data. Indeed, consumer privacy and data innovation are not mutually exclusive.

The NAI is eager to continue working with Congress and other federal policymakers, industry stakeholders, and civil society, in developing workable standards that protect consumers and allow for a vibrant, functioning digital economy.

IX. Conclusion

Again, thank you for the opportunity to comment on this important issue. Please do not hesitate to contact me with any questions or to discuss. The NAI looks forward to further engagement with the Committee and other policymakers as they strive to protect the health data of American citizens.

Respectfully Submitted,

David LeDuc
Vice President, Public Policy
Network Advertising Initiative (NAI)