NAI
PRIVACY, TRUST & ACCOUNTABILITY

2023

Demographic Health Advertising Best Practices

TABLE OF CONTENTS

Introduction

These best practices aim to bolster consumer privacy protection in the area of sensitive consumer health information. At a time when U.S. federal and state laws are evolving, these best practices also help clarify how NAI members can create demographic audience segments that do not rely on consumers' sensitive health information, and that the NAI does not consider to involve inferences about a consumer's health condition, treatment, or diagnosis. Additionally, these best practices provide steps that members can take to protect consumer privacy when modeling de-identified health information.

The legislation and regulation of health-related data use for advertising have expanded dramatically in the last few years and are likely to continue evolving for the foreseeable future. The Federal Trade Commission (the "FTC" or the "Commission") issued a policy statement on the Health Data Breach Notification Rule (HBNR) in 2021,[1] and has since proposed a formal update to the HBNR.[2] The Commission also recently brought enforcement actions regarding sensitive health information against Flo,[3] GoodRx,[4] and BetterHelp.[5] Together, these actions signal the FTC's intent to regulate a broad swath of health-related information. Further, new consumer privacy laws in California,[6] Colorado,[7] Connecticut,[8] Delaware,[9] Indiana,[10] Iowa,[11] Montana,[12] Oregon,[13] Tennessee,[14] Texas,[15] Utah,[16] Virginia,[17] and Washington,[18] present new restrictions and requirements for covered businesses that process consumers' health-related information, including information that is not directly health-related but that may nevertheless "reveal" that a consumer has a given health condition or diagnosis.[19] Indeed, state regulators have even explicitly recognized that *inferences* about a consumer's health status may also constitute sensitive data that requires the consumer's opt-in consent to process.[20] However, these state laws vary significantly in their definitions and scope of sensitive data as it applies to health,[21] and accordingly, members should consult with counsel to determine whether these best practices are applicable in any given jurisdiction that the member may operate in.

The NAI recognizes that health-related information can be among the most sensitive data types, consistent with the 2020 NAI Code of Conduct (Code),[22] which requires a company adhering to the Code to obtain a user's opt-in consent[23] when collecting or using sensitive information[24] for tailored advertising[25] or ad delivery and reporting (ADR).[26] Further, the NAI has long considered sensitive information as defined by the Code to include *inferences* based on web browsing, app use, or other digital content consumption that a user has or is likely to have certain sensitive health or medical conditions. While the NAI Code limits the scope of sensitive health information to, among other things, particularly sensitive health conditions such as cancer, mental health conditions, pregnancy termination, and sexually transmitted diseases, there is little evidence that the regulators responsible for enforcing new privacy laws and regulations will follow the NAI's model by distinguishing between common ailments and those more sensitive conditions.

Because many of the new privacy laws and regulations require opt-in consent to process sensitive data[27] – which, as discussed above, may be interpreted to include a broad swath of health-related information – it is increasingly important to distinguish between the use of sensitive and non-sensitive personal data to create advertising audiences. For example, some audience creation methods that rely on sensitive information (such as health data, purchase

information, or deductive inferences based on a user's prior engagement with a health-related website or mobile application) are likely to require consumer consent under certain new privacy laws; but on the other hand, audience creation methods that rely only on general demographic factors such as age, gender, education level, presence of children or pets in the household, or general geographic region need not involve the processing of sensitive data in a way that requires consumer consent.

For example, a pharmaceutical company may seek to advertise to an audience composed only of men a treatment for a health condition that only (or predominantly) affects men, such as prostate cancer. However, creating an all-male audience for this advertisement does not require processing any sensitive health data about the consumers that constitute the audience, and need not even involve an inference that any particular member of the audience has prostate cancer. Instead, the advertiser is relying on a population-level observation that only (or predominantly) men get prostate cancer and is creating an audience composed of men to increase the likelihood that the treatment being advertised is relevant to the audience. Relying on the population-level insight that only men get prostate cancer does not require the advertiser to assume or infer that any particular member of the target audience has prostate cancer – and anyone making such an inference would be committing a logical fallacy.[28]

Similarly, a hospital may advertise its new treatment center for arthritis to an audience of consumers who are believed to be over sixty years old. Ad targeting based on demographic factors such as age is one way to allow advertisers to reach consumers with ads that may be more relevant to them while at the same time respecting consumer privacy by doing so without processing sensitive data. And, similarly, the advertiser need not infer that any particular member of its audience of 60+ year-olds actually has arthritis. The NAI believes that this approach is analogous to and consistent with the "high level" location or web browsing information that is not considered "sensitive data" under some state laws.[29]

In addition, a website or application publisher may review the non-sensitive demographic composition of its users, and then show related advertisements to consumers with similar demographic characteristics. This is markedly different from showing retargeted ads to the same consumers who actually visited the website or used the application or placing those same consumers in a health-related audience segment for tailored advertising because it does not rely on individual behavior.

Beyond basic criteria for creating health-related audiences, such as the age and gender examples discussed above, it is also possible to learn other population-level demographic insights through analyzing *de-identified* health information, such as insurance claims or pharmaceutical prescriptions. For example, an analysis of de-identified insurance claims data may provide insights into which geographic regions or areas may have an increased prevalence of certain conditions over several years, allowing pharmaceutical companies or healthcare providers to market medications and treatments to consumers in those regions or areas through direct mail, billboards, or digital advertising. Similarly, a company can also use *de-identified* health information to model the demographic characteristics that are most common in the overall population for a given health condition, which may include demographics such as age, gender, geographic region, marital status, household income, and others. *Notably, as race and ethnicity are often considered*

sensitive data under state law,[30] they cannot be used for demographic targeting, modeling, or in the selection of regions for these purposes without first obtaining opt-in consent from the relevant consumers as required by applicable state privacy laws.

The NAI is mindful of the fact that in some cases, if demographic factors relating to a consumer are combined and overlaid with additional information about that consumer -- such as the consumer's health-related web browsing, app use, specific purchases, or precise location information -- such information has greater potential to reveal information about the consumer's health status. Further, with enough specificity and precision, this type of individual behavioral data (*i.e.*, what a consumer views online, what they buy, or where they go) could also support an inference that a user has, or is likely to have, a certain health or medical condition, treatment, or diagnosis. To the extent the use of individual behavioral data does reveal a consumer's health status or is used to make an inference about the consumer's health status, that information may need to be treated as sensitive information.

When the NAI initially released its Guidance for NAI Members: Health Audience Segments in January 2020,[31] it painted broad strokes, addressing national advertising campaigns for more common conditions. In the three years since then, the NAI has gained considerable insight into how to add further consumer privacy-protective measures, while also making it more practical for everyday applications such as regional targeting for various hospitals and health centers. These best practices also increase the viability of advertising for clinical trials and other messaging related to rare conditions falling under the Orphan Drug Act,[32] 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.

These best practices focus only on demographic targeting and modeling, and do not address technical and legal questions related to measurement, attribution, or reporting based on health-related advertising, which the NAI may explore in the future.

These best practices are written for NAI members but may be used by the broader digital advertising ecosystem, including advertisers, retailers, and publishers looking to better understand their own customers and audiences, or to vet vendors who provide demographic audience segments.

Please note that these best practices are not, and should not be taken as, legal advice regarding your compliance with any applicable laws or regulations. The NAI encourages readers who are interested in these best practices to consult with their own legal counsel regarding compliance with laws and regulations in all geographic regions applicable to their business.

I. Demographic Audience Segment Attributes

A. Members should consider the type of audience attributes they use to create and target demographic audience segments for tailored advertising.

1. The NAI does not consider an audience segment that is created based only on demographic attributes such as age, gender, education level, presence of children, or region to reveal, or to be an inference about, a health condition, treatment, or diagnosis of any specific individual in the audience segment.

2. The NAI does not consider individual purchase data (including over-the-counter medications, treatments, or medical devices), historical precise location information, or other individual behavioral data, including historical web browsing or app use directly related to any health condition or treatment, to be demographic attributes.

Commentary: The NAI has refrained from defining the term "demographic" or providing a finite list of acceptable demographic attributes. However, these best practices clarify what types of behavioral information, examples of which are provided above, would not be considered "demographic" by the NAI. Additionally, § V.A of these best practices calls for members to publicly disclose the types of criteria they use to create health-related demographic audience segments in order to provide further transparency around what each member considers to be demographic.

B. Members should not use any demographic attributes about a consumer, such as race or ethnicity, that would themselves be considered sensitive under applicable laws and regulations, to create demographic audience segments for tailored advertising without obtaining that consumer's opt-in consent.

II. Data Stewardship

A. Members should only use, sell, or share demographic health audience segments to or with healthcare or life science companies.

B. Members should employ reasonable due diligence to help prohibit misuse and abuse of health audience segments by recipients.

Commentary: While demographic information may not rise to the level of an inference about a consumer's health condition, members should still exercise care when sharing such information. For example, members should not allow demographic audience segments to be used to target elderly consumers with fraudulent offers, counterfeit prescription drugs, or investment schemes. Members should contractually prohibit such uses, and should take commercially reasonable steps to familiarize themselves with their clients' products and services to help prohibit such uses.

C. When directly executing an advertising campaign that is related to a rare condition under the Orphan Drug Act, or a condition that otherwise would be considered sensitive under the NAI Code of Conduct, members should take steps to limit the frequency of such advertising to an individual device.

Commentary: The NAI does not set specific ad frequency limits, but urges those who are in a position to control this factor to take steps to prevent such ads from being shown to the same consumer too many times, the frequency of which may depend on the seriousness and rarity of the condition and the member's discretion.

III. Modeled Audience Segment Size

A. Members should use reasonable efforts to determine whether a modeled audience segment is large enough to prevent individual members of the audience from being identified with a specific health condition, treatment, or diagnosis. The NAI considers the following modeled audience segment sizes to be adequately large to meet this goal:

1. 10% of the population of a targeted geographic region, with a minimum modeled audience segment size of 100,000; or

2. For rare conditions covered by the Orphan Drug Act, 10 times the prevalence of that condition, as based on reliable sources in the public domain, with a minimum modeled audience segment size of 100,000.

Commentary: To illustrate how this is applied for regional targeting one can consider two cities, City A, with a population of 5,000,000, and City B with a population of 500,000. In City A, the minimum segment size would be 500,000, which is 10% of the city population. However, 10% of the population of City B, or 50,000, would not meet the minimum segment size of 100,000, so the segment would need to include 20% of the population of City B to meet the 100,000 minimum.

	Population	**10% of Population**	**Minimum Segment Size**
City A	5,000,000	500,000	500,000
City B	500,000	50,000	100,000

To illustrate how this is applied to rare conditions, one can consider two conditions, Condition Y affects 150,000 individuals in the United States, which is .04% of the general population, and Condition Z affects 5,000 individuals in the United States, which is .0015% of the total population. For Condition Y, 10 times the prevalence would be a minimum segment size of 1,500,000. However, for Condition Z, 10 times the prevalence, or 50,000, would not meet the minimum segment size of 100,000, so the segment would need to include 20 times the prevalence of the condition to meet the 100,000 minimum. This helps ensure minimum segment sizes and ensures that such segments are not overly precise, while also benefiting society by allowing for more effective campaigns to fill clinical trials for rare conditions.

	Prevalence	**10 x Prevalence**	**Minimum Segment Size**
Condition Y	150,000	1,500,000	1,500,000
Condition Z	5,000	50,000	100,000

IV. Data Provenance

A. Consistent with the Code, members should conduct due diligence to ensure they collect or receive personal information only from partners who comply with applicable laws and regulations, including required consumer notice and choice.

B. When dealing with Health Insurance Portability and Accountability Act (HIPAA)[33]-covered data, members should only ingest data used for modeling or region selection in secure environments, in accordance with HIPAA de-identification requirements,[34] and when relying on expert determination, should publicly demonstrate HIPAA compliance, for example, by posting a letter of confirmation of compliance by a trusted third-party statistician.

Commentary: Because some models may be built by analyzing pharmaceutical prescriptions or health insurance claims, members should ensure the data used to train the model has been de-identified in accordance with the HIPAA standard.

V. Transparency

A. Members should provide transparency into their audience segmentation practices by providing public disclosures of the key criteria used in the modeling or region selection process.

Commentary: This provision is intended to provide transparency into the demographic criteria used by members, without the need to disclose trade secrets or proprietary information. Members can accomplish this by disclosing the types of demographic factors used in the creation of health-related demographic audience segments, such as age, gender, education, presence of children or pets, or others.

B. Members should make reasonable efforts to ensure that marketing materials and segment names clarify that no individual consumer's health-related information is used to create the segments, and that they are based only on demographic information or region.

Commentary: This provision calls for members to take steps to ensure that health-related demographic or regional audience segments are marketed and licensed as such, to prevent misconceptions that those segments may be based on individual consumers' health information, and that those segments do not represent an inference that an individual has any health condition.

Sources

1. Federal Trade Commission, Statement of the Commission On Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021).

2. Federal Trade Commission. FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18, 2023).

3. *FTC v. Flo Health, Inc.* (N.D. Cal.)(2021).

4. *FTC v. GoodRx, Inc.* (C.D. Cal.)(2022).

5. *FTC v. BetterHelp, LLC* (C.D. Cal.)(2021).

6. California Consumer Privacy Act, Cal. Civ. Code §1798.140 (ae)(2)(B).

7. Colorado Privacy Act, Colo. Rev. Stat § 6-1-1303(24)(a).

8. Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(27).

9. Delaware Personal Data Privacy Act, 6 Del. C. § 12D-102(30)(a).

10. Indiana Data Protection Act, IC. § 24-15-2-28.

11. Iowa Consumer Data Protection Act, Iowa Code § 715D.1(26).

12. Montana Consumer Data Privacy Act, S.B. 0384 § 2(24)(a).

13. Oregon Consumer Privacy Act, S.B. 619 §1(18)(A).

14. Tennessee Information Protection Act, Tenn. Code Ann. § 47-18-3201(25).

15. Texas Data Privacy and Security Act, H.B. 4 §541.001(29).

16. Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101(32).

17. Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575.

18. My Health My Data Act, Washington House Bill 1155 (2023).

19. *See, e.g.*, Va. Code Ann. § 59.1-575 (defining "Sensitive Data" to include "a category of personal data that includes . . . personal data revealing . . . mental or physical health diagnosis[.]").

20. *See* 4 Colo. Code Regs. 904-3, Rule 2.02 (setting forth definitions of "Revealing" and "Sensitive Data Inference" specifying that inferences made by a data controller that indicate a consumer's mental or physical health condition or diagnosis "reveal" that consumers health status, and therefore are "Sensitive Data" under the Colorado Privacy Act.")

21. *Compare* Indiana Code § 24-15-2-28 (limiting the scope of health information defined as "sensitive" to "a mental or physical health diagnosis made by a health care provider[.]") *with* Washington HB 1155 § 3(8) (defining "consumer health data" broadly to include any personal information "that identifies the consumer's past, present, or future physical or mental health status[,]" including when such personal information is "derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).").

The difference in scope of covered information illustrated by these two definitions demonstrates why careful analysis is called for as to whether even demographic characteristics taken alone may fall under the broadest definitions of covered health data.

22. *See* Network Advertising Initiative, 2020 NAI Code of Conduct, [hereinafter 2020 NAI Code of Conduct].

23. *See* 2020 NAI Code of Conduct § I.H.

24. *See* 2020 NAI Code of Conduct § I.O.

25. *See* 2020 NAI Code of Conduct § I.Q.

26. *See* 2020 NAI Code of Conduct § I.A.

27. *See*, e.g., Va. Code Ann. § 59.1-578(A)(5) (prohibiting a controller from processing a consumer's sensitive data without obtaining the consumer's consent.)

28. "Affirming the consequent" is a logical fallacy whereby a true conditional statement is used to incorrectly infer the converse of that statement. In this case, it would be fallacious to infer from a true conditional statement such as "if you have prostate cancer, you are likely a man" the converse that "if you are likely a man, then you have prostate cancer." *See https://en.wikipedia.org/wiki/Affirming_the_consequent*.

29. *See* 4 Colo. Code Regs. 904-3, Rule 2.02 (setting forth definitions of "Revealing" and "Sensitive Data Inference" specifying that "high level" precise geolocation and "high level" web browsing data may not be considered "Sensitive Data" under the Colorado Privacy Act.)

30. *See*, *e.g.*, Va. Code Ann. § 59.1-575 (defining "sensitive data" to include "a category of personal data that includes . . . personal data revealing racial or ethnic origin[.]").

31. Network Advertising Initiative, Guidance for NAI Members: Health Audience Segments, January 2020.

32. Orphan Drug Act, Pub. L. 97-414 (1983), available at: https://www.govinfo.gov/content/pkg/STATUTE-96/pdf/STATUTE-96-Pg2049.pdf.

33. The Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. Stat. 1936.

34. *See*, *e.g.*, Office for Civil Rights. (2012, November 26) Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. United States Department of Health & Human Services. Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.