November 2, 2026

*Submitted via electronic mail to auditteam@cppa.ca.gov*

California Privacy Protection Agency
Attn: Audits Division – Request for Input
400 R St., Suite 350
Sacramento, CA 95811

**RE: Technical Input: Emerging Tech**

Dear Audits Division,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide input on the Audits Division's first request for technical input ("RFI") to assist it in developing an audit framework that is both proactive and enables the operationalization of privacy. The NAI applauds the California Privacy Protection Agency's (the "Agency") demonstrated commitment to public engagement and transparency, and particularly its efforts to obtain input from a wide range of stakeholders.

## I. About the NAI

Founded in 2000, the NAI is the leading non-profit, self-regulatory trade association for advertising technology (ad-tech) companies. For 25 years, the NAI has promoted strong consumer privacy protections, a free and open Internet, and enabled small businesses to thrive by promoting the highest voluntary industry standards for the responsible collection and use of consumer data.[1] The NAI has nearly 80 member companies that span the ad-tech industry. Many NAI members are California businesses, and all of them operate in California.

The NAI is committed to helping its member companies not only become aware of evolving regulatory expectations, but be equipped to meet them. Through its privacy review program, the NAI reviews and assesses member adherence to the *NAI Principles & Self-Regulatory Framework* ("NAI Framework") on an annual basis.[2] The NAI also regularly develops best practices and member education resources that translate complex and evolving legal requirements into actionable guidance, helping bridge the gap between regulatory intent and real-world implementation. For example, the NAI recently published its *Factor Analysis for Health-Related Sensitive Personal Information*, a structured tool designed to help businesses and policymakers evaluate when personal information processed in advertising contexts may, or may not, qualify as sensitive health data under U.S. legal frameworks.[3]

## II. NAI Responses to the CalPrivacy Audits Division RFI

The NAI supports the Audits Division's objective to develop an audit framework that will help make compliance more consistent across the industry. The California Consumer Privacy Act ("CCPA") and the

[1] *See* History of the NAI, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.
[2] *See* Privacy Review Program, The Network Advertising Initiative, https://thenai.org/self-regulatory-framework/privacy-review-program/.
[3] *See* NAI's Factor Analysis for Health-Related Sensitive Personal Information, https://thenai.org/wp-content/uploads/2026/02/NAI_Factor-Analysis-for-Sensitive-Health-Information_02242026.pdf.

Delete Act[4] establish important privacy protections, but the application of those provisions to evolving technologies and practices will naturally raise complex interpretive and operational questions.

In responding to this RFI, the NAI is focusing on two questions posed by the Audits Division: (1) what meaningful thresholds are or can be used to distinguish between statistical correlation and actionable sensitive inference? and (2) what are robust and defensible standards for deidentification, including when data is used to train or interact with machine learning models? Our input is summarized below: with additional context and details provided in the subsequent sections.

- The NAI recommends that the Agency recognize a key set of thresholds to distinguish between a statistical correlation and actionable sensitive inference within the context of modeling audience segments for digital advertising.
- The NAI recommends that the Agency treat personal information (separate and aside from *Protected Health Information*) that has been de-Identified using HIPAA's Expert Determination Method as a defensible standard that satisfies the first prong of "Deidentified" under the CCPA.

The subsequent sections provide additional context and details for the Audits Division to consider when developing its audit framework.

### A. What meaningful thresholds are or can be used to distinguish between statistical correlation and actionable sensitive inference? What methodologies best assess whether an inference was "acted on"?

#### i. Introduction to the NAI Best Practices

The NAI appreciates the Agency seeking input to help establish meaningful thresholds to distinguish between statistical correlation and actionable sensitive inference. This is a complex issue, but also an area where the NAI has a long history in promoting industry standards to enhance consumer privacy and reduce the risk of harmful outcomes from processing personal information. The NAI has long recognized that "sensitive personal information" may include traditional personal information when it is used to make specific sensitive inferences.[5] This has been a core principle of the NAI's self-regulatory efforts predating the CCPA.[6] The NAI also has a long history of encouraging members to exercise care in their processing of personal information, providing guidance for processing that avoids the use of sensitive data or making inferences about sensitive data categories, while still enabling uses of the data that can be beneficial to consumers and businesses.[7]

---

[4] *See* Cal Civ Code § 1798.100 et seq. (CCPA); § 1798.99.80 et seq. (Delete Act).

[5] *See, e.g.* Network Advert. Initiative, 2020 NAI Code of Conduct (superseded 2025), https://thenai.org/wp-content/uploads/2021/07/nai_code2020.pdf (defining "Sensitive Information" to include inferences made about a consumer's sensitive health or medical conditions or treatments).

[6] Prior to being superseded in 2025 by the Self-Regulatory Framework, the NAI Code of Conduct was used for decades, with significant updates made in 2013, 2018, and 2020. *See* History of the NAI, https://thenai.org/about-the-nai-2/history-of-the-nai/; Principles & Self-Regulatory Framework, https://www.thenai.org/wp-content/uploads/2025/03/NAI-Framework_March-2025.pdf.

[7] *See generally Guidance for NAI Members: Health Audience Segments, Network Advertising Initiative (Jan. 2020)*, https://thenai.org/wp-content/uploads/2021/07/nai_healthtargeting2020.pdf; Factor Analysis for Health-Related Sensitive Personal Information, https://thenai.org/wp-content/uploads/2026/02/NAI_Factor-Analysis-for-Sensitive-Health-Information_02242026.pdf; *Demographic Health Advertising Best Practices* (2023), https://thenai.org/wp-content/uploads/2023/11/NAI-Health-Targeting-Best-Practices-Document-Final.pdf.

The NAI has developed two guidance documents that are particularly relevant to the Audits Division's RFI, as they are useful for making distinctions about what types of data may rise to the level of sensitive health information (including the use of sensitive inferences). The first is a set of best practices aimed at helping digital advertising businesses create demographic audience segments without utilizing sensitive data or making sensitive inferences. Known as the NAI's *Demographic Health Advertising Best Practices* ("Best Practices"), these are relevant to the Audits Division's question because they establish thresholds that businesses can apply to effectively reach audiences with relevant advertising without the need to make a sensitive inference about a particular consumer, such as their health status (more on this below).[8]

The second is the NAI's *Factor Analysis for Health-Related Sensitive Personal Information* ("Factor Analysis"), a structured tool designed to help NAI member companies and other businesses make a thoughtful determination as to whether a particular data type, or inference made from the data, rises to a level of being classified as sensitive personal information. Especially as the CCPA defines sensitive personal information to include "[p]ersonal information collected and analyzed concerning a consumer's health,"[9] this analysis can be challenging within the context of digital health advertising, where one use case of personal information may have nothing to do with a consumer's health, and another use case involving the same personal information may draw a health-related sensitive inference about a consumer depending on the context.[10] We therefore hope the NAI's resources are useful to the Audits Division for analyzing digital advertising use cases that can be achieved without making sensitive inferences. The NAI developed these industry guidance documents with the goal to preserve responsible data-driven health advertising, which has been demonstrated to improve public health equity and outcomes, as we discuss in the following section.

### ii. Data-driven health advertising benefits health outcomes

Data-driven health advertising and marketing has been demonstrated to enhance the ability to reach underserved populations, provide an overall increase in patient engagement and treatment adoption, and improve overall health outcomes. The NAI recently published a comprehensive resource that compiles data to demonstrate how tailored digital health advertising produces measurable positive health outcomes including more than 60 measured findings from health campaigns run by various groups, including federal agencies, nonprofits, and medical associations.[11] The peer-reviewed literature and other research finds that tailored health messages produce significant beneficial outcomes, including smoking cessation, increased vaccination rates, and cancer screening.[12] A randomized trial of 794,000 people found that tailored health ads significantly increased health information seeking, a

---

[8] *See generally* Network Advertising Initiative, *Demographic Health Advertising Best Practices* (2023), https://thenai.org/wp-content/uploads/2023/11/NAI-Health-Targeting-Best-Practices-Document-Final.pdf.

[9] *See* Cal. Civ. Code § 1798.140(ae).

[10] *E.g*. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Mag. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (describing how Target combined purchases of roughly 25 ordinary products to assign shoppers a "pregnancy prediction" score); *see also* Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Nw. U. L. Rev. 1081 (2024) (arguing that modern data processing allows non-sensitive personal data to give rise to sensitive inferences, such that sensitivity depends on how data is used rather than on the data itself).

[11] whydigitaladvertising.org.

[12] *See e.g.* Mia Liza A. Lustria et al., *A Meta-Analysis of Web-Delivered Tailored Health Behavior Change Interventions*, 18 J. Health Commc'n 1039 (2013) (finding that web-delivered tailored interventions produced statistically significant improvements in health behaviors compared with control conditions).

validated indicator of later health action.[13] The most important findings related to federal health advertising campaigns include the following, which were created to reach specific key at-risk audiences, without relying on sensitive inferences:

- **U.S. Center for Disease Control (CDC), *Tips From Former Smokers*:** an estimated 129,000 early deaths prevented between 2012 and 2018, saving about $7.3 billion in healthcare and related costs.[14]
- **U.S. Department of Health and Human Services, *We Can Do This* (COVID-19 vaccination):** an estimated 51,000 lives saved and nearly 244,000 fewer hospitalizations in the campaign's first year, with about $90 in healthcare savings per dollar spent.[15] First-dose vaccination among Black participants rose from 30% at the start of the campaign to nearly 80% by its end, helping narrow health disparities.[16]
- **U.S. Food and Drug Administration (FDA), *The Real Cost*:** $180 in reduced healthcare costs per $1 spent over the first two years, and an estimated 450,000 young people kept from starting e-cigarettes in 2023–2024.[17]

These federal campaigns show why the government itself relies on data-driven health advertising to improve health outcomes, and these use cases demonstrate that responsible targeting based on non-sensitive data also preserves privacy. The same data practices that let these campaigns reach their audiences are the ones that overly broad restrictions on health-related advertising would put at risk.

### iii. Health advertising that uses demographic targeting

In reaching audiences with health advertising and messaging that is more likely to be relevant, many companies seek to avoid processing sensitive personal information or making sensitive inferences. Instead, these companies rely on non-sensitive demographic observations about a population to increase the relevance of the health messaging. For example, an ad-tech company may assist a healthcare provider with advertising to an audience composed only of men for a treatment for prostate cancer, a health condition that only (or predominantly) affects men, and has the highest number of new

---

[13] *See* Elad Yom-Tov et al., *The Effectiveness of Public Health Advertisements to Promote Health: A Randomized-Controlled Trial on 794,000 Participants*, 1 npj Digit. Med. 24 (2018), https://doi.org/10.1038/s41746-018-0031-7.

[14] *See* CDC, *Tips From Former Smokers® Campaign Impact and Results*, CDC Campaign (Oct. 8, 2024), https://www.cdc.gov/tobacco/campaign/tips/about/impact/campaign-impact-results.html.

[15] *See* Sidney Turner et al., *Association of a COVID-19 Vaccination Public Education Campaign With Vaccination Uptake and Health Outcomes in the U.S.*, Am. J. Preventive Med., Volume 67, Issue 2 p. 258-264 (Aug. 2024), https://www.ajpmonline.org/article/S0749-3797(24)00110-7/fulltext.

[16] Joseph N. Luchman, Association Between the United States Department of Health and Human Services' COVID-19 Public Education Campaign and Initial Adult COVID-19 Vaccination Uptake by Race and Ethnicity in the United States, 2020–2022, Health Promotion Practice (Dec. 30 2023), https://journals.sagepub.com/doi/10.1177/15248399231221159.

[17] *See e.g.* U.S. Food & Drug Admin., FDA Educational Efforts Prevented Nearly 450,000 Youth from Starting E-Cigarette Use in One Year (Mar. 14, 2025), https://www.fda.gov/news-events/press-announcements/fda-educational-efforts-prevented-nearly-450000-youth-starting-e-cigarette-use-one-year (reporting that "The Real Cost" youth cigarette prevention campaign saved $180 for every dollar spent in its first two years, totaling more than $53 billion in reduced smoking-related costs); *see generally* The Benefits of Digital Health Advertising, https://www.whydigitaladvertising.org/.

diagnoses among those aged 55-69 years old.[18] Creating an audience with those demographic characteristics for this advertiser increases the relevance of the messaging and increases the likelihood that it will reach consumers that would benefit from more information about prostate cancer. However, creating this audience neither requires processing any sensitive personal information about the consumers that constitute the audience, nor does it require processing personal information to make a sensitive inference. Instead, the advertiser is relying on a population-level observation that men 55-69 years old account for more than half of new prostate cancer diagnoses. This is a common approach to increasing the likelihood that the advertisement is relevant to an audience without assuming or inferring that any particular member of the target audience has a specific health condition or inferring any other sensitive conclusions about target audience members. The 52% figure describes where new diagnoses occur; it does not mean that any individual man in that age group has a 52% chance of being diagnosed.

Beyond basic criteria for creating health-related audiences, such as the age and sex example discussed above, other population-level demographic insights can be learned about the prevalence of health conditions by analyzing de-identified health information, such as insurance claims data that has been de-identified under the *Health Insurance Portability and Accountability Act* (HIPAA). For example, a business may use de-identified health information to model the non-sensitive demographic characteristics[19] that are most common in the overall population for a given health condition.[20]

#### iv. The NAI's Best Practices provide useful thresholds to distinguish between a statistical correlation and an actionable sensitive inference within the context of modeling audience segments for digital advertising

Within the context of modeling an audience segment for data-driven advertising, the NAI recommends the Agency consider the following thresholds from the NAI Best Practices to distinguish between a statistical correlation and an actionable sensitive inference:

---

[18] *See* Center for Disease Control & Prevention, Prostate Cancer Incidence (Sept. 25, 2025), https://www.cdc.gov/united-states-cancer-statistics/publications/prostate-cancer.html (reporting that, in 2022, 52% of prostate cancer cases were diagnosed among men aged 55 to 69, compared with 43% among men aged 70 or older and 5% among men aged 45 to 54).

[19] Notably, as data revealing race and ethnicity are considered sensitive personal information under the majority of comprehensive state privacy laws, including the CCPA, this personal information would normally not be used for demographic targeting or modeling without first obtaining opt-in consent from the relevant consumers. *See, e.g.* Colo. Rev. Stat. § 6-1-1308(7) (2025) (prohibiting controllers from processing sensitive data without first obtaining the consumer's consent); Conn. Gen. Stat. § 42-520(a)(1)(D) (2026); Tex. Bus. & Com. Code Ann. § 541.101(b)(4) (West 2025); *but see* Cal. Civ. Code § 1798.121 (West 2025) (granting consumers a right to limit a business's use and disclosure of sensitive personal information rather than requiring prior consent); Utah Code Ann. § 13-61-302(3)(a) (West 2025) (requiring only that controllers present clear notice and an opportunity to opt out before processing sensitive data); Iowa Code § 715D.4(2) (2025).

[20] For example, an ad-tech company may analyze de-identified insurance claims data to better understand the demographic characteristics of a population who has already been prescribed a particular diabetes medication. This analysis results in insights that the population that has already purchased the drug is more likely to be over age 65 and have an annual income <$25,000, making that demographic an audience that the drug is more likely to be relevant to. The ad-tech company then obtains a set of targetable device IDs associated with consumers who match those demographic criteria from a data partner that lawfully obtained that information from public records and survey data, and runs an advertising campaign for that medication. *See generally NAI's Factor Analysis for Health-Related Sensitive Personal Information* at 15–17 (Hypothetical #3), https://thenai.org/wp-content/uploads/2026/02/NAI_Factor-Analysis-for-Sensitive-Health-Information_02242026.pdf.

1. Audience size – When modeling an audience segment to ensure individual members of an audience are not identified with a specific health condition, the audience segment should include at least 10% of the population of a targeted geographic region, with a minimum modeled audience segment size of 100,000;[21] or for rare conditions, ten 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.[22]

2. Audience Labeling – Marketing materials and audience segments should take care not to suggest that members of the audience have any specific medical conditions.

3. Data Stewardship – Employ reasonable due diligence to help prohibit misuse and abuse of audience segments by recipients.

4. Audience composition disclosure – Publicly disclose criteria used to create demographic audience segments that explain how these were created without the use of sensitive personal information.

Under these conditions, if a modeled audience segment must include at least 10% of a geographic region's population (or 10x the prevalence of a rare condition), with a hard floor of 100,000 individuals, then membership in that segment would not give rise to an opportunity to meaningfully identify any individual as having a specific health condition. In other words, the segment is derived from a population-level observation, composed of individuals who are more likely to have an interest in a specific health topic or treatment, rather than a sensitive-inference about any of the particular individuals in that segment.

We also recommend these thresholds for evaluating audience segments because they are easily auditable. That is, an auditor would not need to examine the complexities of model internals or algorithmic processes; they would simply need to verify whether the advertising segment meets the established quantitative and qualitative thresholds while also following certain transparency and audience labeling best practices.[23]

This approach is inherently different from the probabilistic inferences described in the RFI, where a calculated sensitive inference about an individual, such as a pregnancy prediction score, raises legitimate privacy concerns because it is based on an identifiable consumer, which creates a heightened level of data processing risk. The NAI Best Practices take a distinctly different approach. Rather than assigning a probability score to individuals or drawing conclusions that any individual has or is likely to have a specific health condition, this approach relies on non-sensitive demographic observations about a

[21] 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.

[22] *See* 21 U.S.C. § 360bb(a)(2), ("For purposes of paragraph (1), the term "rare disease or condition" means any disease or condition which (A) affects less than 200,000 persons in the United States, or (B) affects more than 200,000 in the United States and for which there is no reasonable expectation that the cost of developing and making available in the United States a drug for such disease or condition will be recovered from sales in the United States of such drug.").

[23] The NAI is not suggesting that this method for modeling an audience segment is the only method that does not involve processing sensitive personal information. Segments built using other methods should be assessed on a case by case basis.

population to increase the relevance of certain kinds of health advertising and marketing. Using this approach allows for inferences to be drawn about a consumer that are non-sensitive, as they would pertain to demographic categories of personal information that the CCPA does not designate as sensitive.

This also answers the RFI question of how to assess whether an inference was *acted on*: when no inference about an individual's health is made, there is none to act on. Evidence would show that the segment's inputs are limited to demographic attributes and that the system assigns no health attribute or probability score to any user. For these reasons, we encourage the Audits Division to consider the NAI's Best Practices and Factor Analysis when developing an audit framework.

**B. What are robust and defensible standards for deidentification, including when data is used to train or interact with machine learning models?**

**i. The Audits Division should treat data that has been de-identified using HIPAA's Expert Determination Method as a robust and defensible standard that satisfies the first prong of "Deidentified" under the CCPA**

As noted above, some businesses process de-identified health information, such as insurance claims data that has been de-identified under HIPAA, to generate insights about how demographics correlate to the prevalence of health conditions in a population. To enable this type of advertising, businesses have long relied on the HIPAA standard for de-identifying covered health data.

HIPAA provides two pathways for de-identifying health data: the *Safe Harbor method*, which requires the removal of eighteen categories of direct identifiers,[24] and the *Expert Determination method*, which requires a qualified expert to certify that the risk of re-identification is "very small" given the information and what could reasonably be combined with it.[25] The Expert Determination method involves a rigorous analysis by an expert to assess re-identification risk contextually, accounting for what data is reasonably available that could be combined with the de-identified dataset to identify individuals.[26] Most importantly, this analysis requires considering anticipated recipients of data and their own technological

[24] *See* 45 C.F.R. § 164.514(b)(2) (2025).

[25] *See id.* at § 164.514(b)(1) (providing that health information is not individually identifiable where "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) [a]pplying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) [d]ocuments the methods and results of the analysis that justify such determination"); *see also* U.S. Dep't of Health & Hum. Servs., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule § 2.3* (Nov. 26, 2012) (explaining that "[t]here is no explicit numerical level of identification risk that is deemed to universally meet the 'very small' level," and that the appropriate level depends on the data and the environment in which it will be disclosed).

[26] *E.g.* Williamson & Mosquera, *A More Practical Approach to HIPAA Expert Determination* (June 10, 2026), Datavant (introducing a new structured contextual privacy framework for HIPAA Expert Determination that is designed to be: (1) transparent supported by clear documentation of inputs, assumptions, and models; (2) consistent, enabling repeatable application across similar use cases; (3) grounded, aligning with HIPAA's Expert Determination standard and based on robust statistical and scientific principles).

prowess.[27] Further, according to the text of the CCPA, patient information that has been de-identified according to the requirements of HIPAA is outside the scope of the law.[28]

The CCPA also acknowledges the value and privacy-protective nature of de-identified data by defining the term and explicitly excluding de-identified data from the definition of personal information.[29] For data to be "deidentified," it must satisfy three prongs, with the first requiring that the business take "reasonable measures to ensure that the information cannot be associated with a consumer or household."[30] The NAI recommends the Agency treat any personal information subject to CCPA that has been de-identified using the same processes described under HIPAA's Expert Determination Method as a defensible standard that satisfies the first prong of "Deidentified" under the CCPA.

In line with this approach, the NAI encourages the Agency to judge reidentification risk by the means and technical ability the authorized processor actually possesses, not by what an unknown third party could theoretically do. Similarly, the NAI also encourages the Agency to judge standards by their ability to reduce the risk of re-identification to be insignificant in practice, without an expectation that the risk be reduced to zero.[31]

**ii. A robust and defensible standard for deidentification must also include contractual requirements, such as a prohibition on linking data in such a way that it could lead to reidentification**

The NAI also encourages the Audits Division to include contracts as part of its standard. Especially as reidentification risk within the context of advertising usually arises from improper data linkage as opposed to analysis of a single dataset, a defensible standard should include contractual prohibitions on linking the data in a way that it could lead to reidentification. This approach is also well-aligned with the CCPA, which requires contractually obligating the recipients of de-identified data to comply with the three-prong requirements outlined in the definition.

In practice, an auditor can look for evidence that a business: (1) takes reasonable measures to ensure that the information cannot be associated with a consumer or household, which can include applying

---

[27] *See* 45 C.F.R. § 164.514(b)(1)(i) (requiring that a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable to apply such principles and methods to determine that the risk is "very small" that the information could be used to identify an individual, considering, amongst other things, the anticipated recipient of the data).

[28] *See* Cal. Civ. Code § 1798.146(a)(4)(A) (providing that the CCPA "shall not apply to" information that is "deidentified in accordance with the requirements for deidentification set forth in Section 164.514" of Title 45 of the Code of Federal Regulations and that is "derived from patient information that was originally collected, created, transmitted, or maintained by" an entity regulated by HIPAA, the Confidentiality of Medical Information Act, or the Common Rule); *see also* § 1798.185(a)(2) (providing that the agency's "authority to update the definition of 'deidentified' shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was 'protected health information'").

[29] *See id.* at § 1798.140(v)(1), (3) (defining "personal information" as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," but excluding "consumer information that is deidentified or aggregate consumer information").

[30] Cal. Civ. Code § 1798.140(m).

[31] *See* U.S. Dep't of Health & Hum. Servs., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule § 2.3* (Nov. 26, 2012) (explaining that both methods of de-identifying data under HIPAA reduce the risk of reidentification to be "very small" while acknowledging that the risk is not zero).

the expert determination method used in HIPAA to the data; (2) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information; and (3) contractually obligates recipients to comply with the CCPA's deidentification requirements, including prohibitions on reidentification. Taken together, this creates a complete, auditable standard for digital advertising that satisfies the CCPA's definition of "deidentified."

## III. Conclusion

As noted above, the NAI and its members support the goal of the Audits Division to develop an audit framework and compliance inquiry functionalities. We also look forward to responding to future Requests for Input issued by the Audits Division and serve as a helpful resource where possible.

If we can provide any additional information, or otherwise assist your office as it continues to develop an audit framework that can withstand modern breakthroughs in technology, please do not hesitate to contact me at nick@thenai.org.

Sincerely,

Nick Meyer
Privacy Counsel
Network Advertising Initiative