



Veeva Crossix

The Future of Audience Targeting for Health Brands

February 2020

Contributors



Anthony Matyjaszewski

VP, Compliance and Membership,
Network Advertising Initiative (NAI)

Anthony leads the NAI's annual compliance reviews of member companies, in addition to overseeing updates to the NAI's Code of Conduct and guidance documents.



Lauren Dubick

Director, Senior US Data Privacy Counsel,
Novartis

Lauren leverages her background as a software engineer to develop innovative, privacy-centric solutions, and she advises regularly on privacy best practices and technology design.



Jeremy Mittler

VP, Industry Solutions,
Crossix

Jeremy leads the company's privacy team and is involved in Crossix's commercial activities and strategic discussions.

DISCLAIMER

The views expressed in this ebook are the personal views of the speakers and should not be understood or interpreted as being made on behalf of, or reflecting the position of, their respective companies. Views are presented solely to aid discussion and should not be interpreted as company policy, guidance, or legal advice.

Executive Summary

With the increasing focus on privacy across the healthcare industry, executives from Crossix, the Network Advertising Initiative, and Novartis joined together to educate healthcare advertisers during a November 2019 webcast. They sought to explain current privacy issues in audience targeting and how new guidelines affect and assist advertisers in their work. This ebook is based on that webcast.

Key Takeaways



Knowing how to handle data responsibly is a vital role for everyone in advertising today.



Understanding privacy concerns, policies, and regulations is more important than ever; simultaneously, the landscape is also more complex than ever before.



Being able to confidently create campaigns that ensure privacy enables greater innovation and more effective work.

Audience Targeting in Healthcare

Consider a poet's sonnet. It's a tightly controlled, restricted form of expression, in which the rules must be followed very specifically in order for the art to be considered successful. Our work isn't Shakespeare, but the similarity is there: in order to be effective, we must be extremely creative within a strictly regulated environment.

Heightened privacy concerns, new policies, and regulations have been in the spotlight in 2019, prompting organizations to react. As the public came to understand how much of their individual information exists online, companies scrambled to address data breaches, government authorities sought to codify and regulate the ever-changing world of online data, and smart advertisers worked to stay abreast of evolving restrictions.



A decade ago, HIPAA was the only standard used to regulate healthcare data, and privacy was the responsibility of the privacy team. Now, any stakeholder in messaging to patients has a responsibility – and a competitive advantage – if they understand both the business needs and the privacy elements.

JEREMY MITTLER

In this evolving ecosystem, one thing is clear: advertisers who understand data privacy have better campaign ideas and execute them more effectively. The process of using data to target advertisements through television, the internet, and the overlapping media middle ground is complex and constantly evolving. Originally, guidance on how to protect patient data came only from the 1996 Health Insurance Portability and Accountability Act (HIPAA). As technology advanced, the need for updated guidance became clear, and increasingly, organizations and governing bodies stepped in to provide additional oversight, recommendations and requirements.

In addition to organizations, like the NAI and the Digital Advertising Alliance, regulations, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Federal Trade Commission's Fair Information Practices have created structure around how data is managed.



When you understand the guardrails, innovation becomes possible.

LAUREN DUBICK

Unique Concerns of Healthcare Data

Health-related sensitive information could be obviously direct data, such as a prescription or a diagnosis, which is covered under HIPAA and requires an opt-in consent to be used for advertising. But it could also include inferences based on browser or app use. Inferential data like this is still healthcare data and still has privacy components.

Furthermore, consider how certain conditions or diagnoses can seem to the average person. Novartis's Lauren Dubick calls this the "drugstore test": if you ran into a colleague in a drugstore while holding medicine to treat that condition, would you feel uncomfortable? But even that rule of thumb may have exceptions, as the NAI's Anthony Matyjaszewski pointed out: for instance, while baldness may be an innocuous topic of discussion for many men resigned to the common condition, it might be an extremely sensitive one for a woman.



The higher-level question always is: Is this the right thing to do? Does this engender trust or undermine trust? There has to be trust between the company and its digital stakeholders.

LAUREN DUBICK

About the NAI and the NAI Code of Conduct



We seek to strike a good balance between preserving a thriving internet and maintaining a focus on data minimization and consumer privacy.

ANTHONY MATYJASZEWSKI

The NAI is the leading self-regulating body for digital advertising. Founded in 2000, the non-profit organization (which includes companies such as Adobe, Google, and Microsoft among more than 100 members) seeks to preserve a thriving internet while setting high standards that focus on protecting consumer privacy, in addition to educating and empowering both members and the public. The first version of the NAI Code of Conduct was created

in its founding year, and the document has been updated throughout the years in keeping with the rapid increase and evolution of digital advertising. The Code governs the Tailored Advertising and Ad Delivery and Reporting activities of member companies.

The 2020 NAI Code of Conduct moves for the first time into offline data — a necessary change, in a world where it is far easier than ever before to match database information to mobile IDs and use offline data for online ad targeting. It prohibits any non-marketing use of advertising data (for instance, the denial of health insurance based upon browser behavior or app use). It also incorporates previously separate guidance, adds new definitions and revises others, establishes transparency requirements related to political campaigns, and expands opt-in consent requirements for certain kinds of data.

Types of Consumer Data

The NAI recognizes three types of sensitive consumer data. The type of the sensitive data, and what it will be used for, determines the responsibilities and obligations of advertisers.

1

Personally Identified Information (PII)

This is real-world information that can be used to directly identify a person, such as their name, email address, or Social Security number.

2

Device-Identified Information (DII)

This is information that is linked to a browser or device – attached to a mobile advertising ID on a phone, a cookie ID on a browser, or an ID on a TV, or an ID that links some or all of those, but is not used or intended to be used to directly identify an individual.

3

De-Identified Information

This is data that is not linked or linkable to either an individual or a device.

Healthcare-related Stipulations in the 2020 NAI Code of Conduct

The NAI helped to form the Digital Advertising Alliance in 2010, and the DAA Principles form another set of industry self-guidance. In some ways, however, the NAI Code obliges its members to meet higher standards than those set by the DAA Principles, including submitting to an annual compliance review. In addition, healthcare-related obligations for NAI members include:

- Transparency with respect to all standard “health-related” interest segments used for Tailored Advertising
- Opt-in consent requirements for the use of “sensitive” health segments for Tailored Advertising and Ad Delivery and Reporting

The 2020 NAI Code of Conduct provides guidance related to all facets of digital advertising: the technology used by advertisers, the viewing tools used by the audience, the information gathered, the tailoring approach taken, and more. In some cases, the Code specifies healthcare-related

stipulations for its advertisers. These include specific guidelines for sensitive information. In addition to data, like Social Security Numbers or financial account numbers, sensitive information includes:

- “Information about any past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history, based on, obtained or derived from pharmaceutical prescriptions or medical records, or similar health or medical sources that provide actual knowledge of a condition or treatment (the source is sensitive).”
- “Information, including inferences, about sensitive health or medical conditions or treatments, including but not limited to, all types of cancer, conditions predominantly affecting or associated with children and not treated with over-the-counter medication, mental health-related conditions, and sexually transmitted diseases (the condition or treatment is sensitive regardless of the source).”

To provide additional guidance for health marketers, the NAI published new Guidance for NAI Members: Health Audience Segments in January 2020. In it, they explain that the collection and use of sensitive information requires advertisers to get opt-in consent from users.

Sensitivity can be determined both by whether the source is considered sensitive (e.g. medical records), as well as whether the condition is considered sensitive, regardless of the source (e.g. sexually transmitted diseases, mental health conditions, or pediatric conditions treated by prescription medication).

An audience that is created based only on demographic attributes, such as age, gender, education level, neighborhood affluence, or residence in a broad geographic region, would be an appropriate use of non-sensitive data for Tailored Advertising and Ad Delivery and Reporting by the NAI. Similarly, the use of offline marketing segments that are modelled themselves, and are not based

on any user-level purchase, behavior, or activity, would also be permitted by the NAI.

However, the use of non-demographic attributes such as purchase data, including over-the-counter medications, residence more precise than ZIP-level, or other user-level historical data, would require opt-in consent under the 2020 NAI Guidelines.

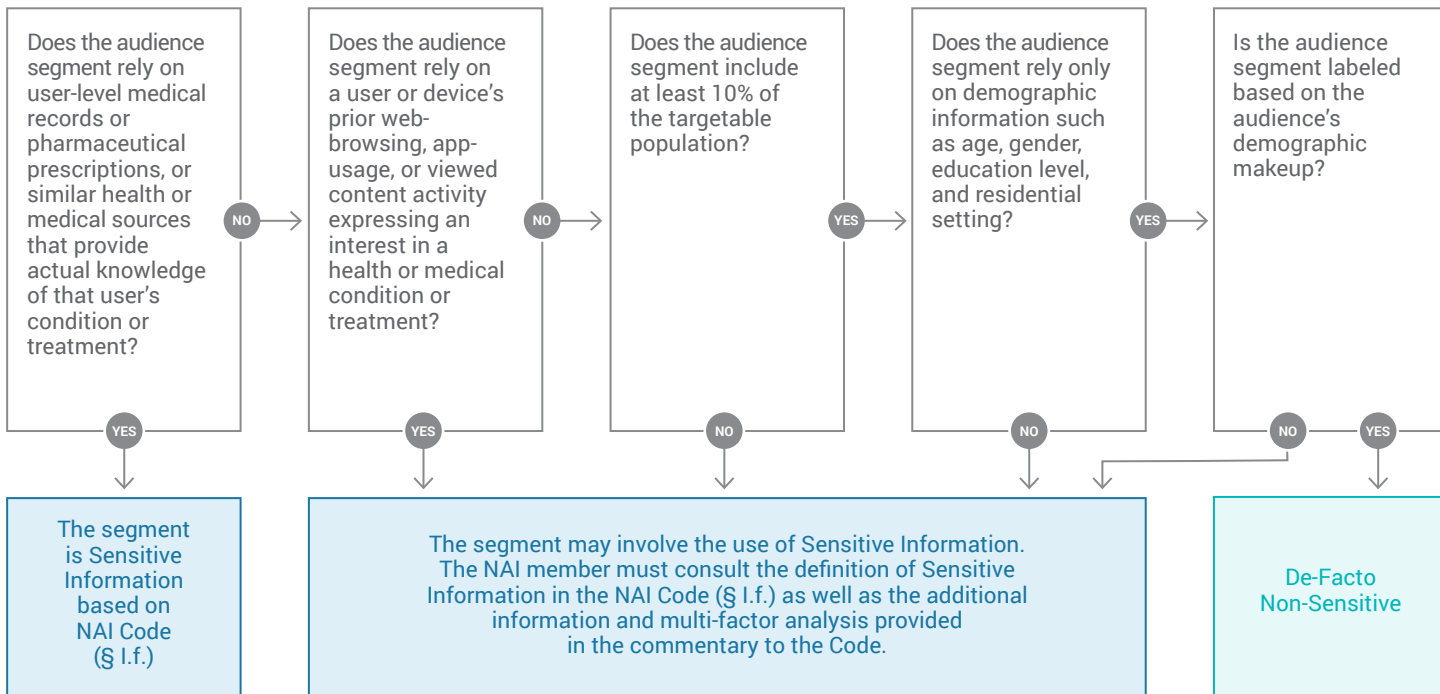


Targeting based on actual health data is prohibited under the 2020 NAI Code, even if additional data noise is added to the targeting segments.

ANTHONY MATYJASZEWSKI

How to Determine Whether a Health-Related Audience Segment is De-Facto Non-Sensitive

If a health targeting segment includes Sensitive Information, it requires a user's opt-in consent.



Source: NAI Guidance for NAI Members: Health Audience Segments, Jan. 2020, Appendix A

Conclusion

Privacy issues were once an afterthought, the realm of a specialized group of individuals that would be contacted to “check the box” at the end of the development of a campaign. Today, that’s no longer the case. Privacy concerns aren’t for a few people in the legal department. They’re front and center for any smart advertiser, and those who know the most about safeguarding consumer privacy – and work with partners who do – are able to come up with the most creative and effective ideas.

In general, the level of choice that advertisers should provide to consumers is commensurate with the sensitivity and intended use of the data in question. But as experts from the NAI, Novartis, and Crossix agreed, there is little black and white in this space: it’s a gray area with lots of shades of gray.

The complexity of healthcare situations means that those campaign designs and determinations are best done by, and with, those with extensive expertise in both data privacy and healthcare. As our experts agreed, the best marketers

use their knowledge of the space and combine it with a constant focus on a fundamental question: Is this the right thing to do? In any conversation about the value of data in advertising, the most precious commodity is always trust between the company and the consumer.



Because we’re able to see meaningful patterns by analyzing massive amounts of information across our data network, Crossix has a better understanding of the consumer profile of potential patients. Leveraging those consumer attributes to build enhanced demographic targeting models improves the likelihood that the ads will reach a relevant audience.

JEREMY MITTLER

Take Action

How can you ensure that your work uses data responsibly?

- Understand the principles of data privacy and the regulations and guidance that apply to your brands.
- Ensure that your campaigns are as innovative and compliant as possible by choosing partner organizations that have been built with privacy in mind from the beginning.
- Beware of shortcuts or “after-market” work-arounds that less scrupulous providers may use to cover noncompliant practices, such as adding extra noise to audience targeting after using health data.
- Often, solution providers may not fully grasp the ramifications of working in healthcare. Or, drug makers may not be fully versed in the latest in ad tech. Seek out experienced partners who put data privacy first, who have industry accolades and demonstrable results in doing so, and who understand both the technology and the industry.
- To find out more about the NAI, visit [Networkadvertising.org](https://www.networkadvertising.org).
- To find out more about Crossix and how we build our health audience segments, visit [Veeva.com/products/audience-solutions](https://veeva.com/products/audience-solutions).



About Veeva Systems

Veeva is the global leader in cloud software for the life sciences industry. Committed to innovation, product excellence, and customer success, Veeva serves more than 1,100 customers, ranging from the world's largest pharmaceutical companies to emerging biotechs. As a Public Benefit Corporation, Veeva is committed to balancing the interests of all stakeholders, including customers, employees, shareholders, and the industries it serves. For more information, www.veeva.com.

Veeva Systems

Global Headquarters
Pleasanton, California, USA
4280 Hacienda Drive
Pleasanton, California 94588
+1 925 452 6500 | veeva.com/contact | veeva.com