May 7, 2025

The Privacy Challenges and Opportunities Presented by Health-Related Advertising

Robyn Eckerling
Tempus

Tony Ficarrotta
NAI

Ben Chapman
Swoop

Ali Jessani
WilmerHale

Privacy+ Security Forum

Speakers

Ali Jessani

Counsel
Cybersecurity and Privacy
WilmerHale

Ben Chapman

General Counsel &
Chief Privacy Officer
Swoop

Robyn Eckerling

Chief Privacy Officer
Tempus

Tony Ficarrotta

Vice President & General Counsel
Network Advertising Initiative

Overview

Overview

- Health-related advertising provides numerous benefits to consumers, including raising public awareness and educating individuals about healthcare options and preventative measures; recruiting for clinical trials; and assisting with payment options
- However, it has become more challenging in recent years given:
  - Emphasis by regulators on pixels and other web trackers
  - New laws governing non-HIPAA health data
  - Increased litigation riskExemption for de-identified data (subject to specific de-identification standards)
- Practical and operational challenges across the industry
- Advertising networks, publishers, and other players in the health-advertising industry have had to update their compliance practices to account for these new legal requirements
- This has created challenges for industry and required creative solutions

Topics

Topics

1. Overview of applicable regulatory framework
2. Strategies and considerations
    a. De-identification
    b. Demographic vs. Health Data
    c. Collaboration between stakeholders
3. Key takeaways

Overview of Regulatory Framework

Privacy+ Security Forum

HIPAA

- Applies to covered entities (healthcare providers, health insurers, and healthcare clearinghouses) and their business associates (e.g., service providers)
- Creates specific rules for how covered entities are permitted to use protected health information
- Relevant concepts for targeted advertising:
  - Broad definition of PHI
    - Exemption for de-identified data (subject to specific de-identification standards)
  - Permitted purposes
    - Treatment, payment, operations do not require additional consent
    - Other purposes/disclosures require a specific authorization
  - Marketing Rule
    - Additional exemptions for specific marketing activities
  - Contractual restrictions on business associates
    - Specific permission required for de-identification

State Comprehensive Privacy Laws

- 19 states have passed "comprehensive" privacy laws that create general data processing obligations for controllers/businesses
  - Subject to a number of exemptions, including data-level and entity-level exemptions for HIPAA
  - Also include exemptions for de-identified and aggregated data (subject to specific standards)
- These state laws create certain compliance obligations that are relevant to health-related advertising
  - Opt-out of sale/targeted advertising
  - Data protection impact assessments
  - Privacy notice requirements
- A number of the state laws have unique requirements:
  - CCPA - Do Not Sell or Share
  - Maryland - strict data minimization requirements (goes into effect in October)
  - Delaware - specific due diligence for de-identified data

State Consumer Health Data Laws

- Few states have passed laws specifically regulating “consumer health data”, most notably Washington’s My Health My Data Act (MHMDA)
- MHMDA is notable for a few reasons:
  - Broad definition of consumer health data (includes inferences drawn from nonhealth data)
  - Specific authorization required for “selling” consumer health data
  - Private right of action
- Other states:
  - Nevada has passed a similar to MHMDA (without a PRA)
  - Number of state comprehensive privacy laws have incorporated “consumer health data” within their scope of “sensitive data” (e.g., CT and MD)
  - NY is considering a similar law (HIPAA; with the governor for signature)
  - VA signed into law a reproductive data health bill (that includes a PRA)

Other Relevant Legal Frameworks

- FTC
  - Unfairness authority under Section 5
  - Health Breach Notification Rule
- State Wiretapping Laws
  - CIPA litigation
- State Data Broker Laws
  - California, Vermont, Oregon, and Texas
- DOJ Data Transfers Rule
  - Creates specific requirements for data transfers to covered persons or countries of concern (including China)
  - Prohibits certain transactions (including those tied to data brokerage)
  - Broad definition of data brokerage (would apply to data disclosures for certain advertising purposes)
  - Civil and criminal liability
  - No exemption for de-identified data

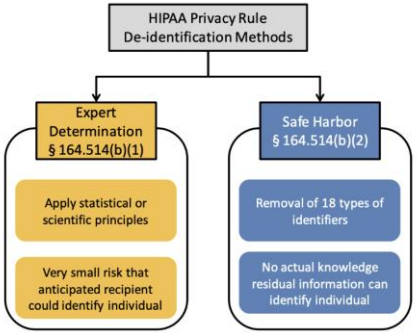
Strategies and Considerations

Privacy+ Security Forum

De-identification

- **De-identification** refers to the process of removing or altering direct and indirect identifiers from an information set such that it cannot reasonably be used to identify an individual - "breaking the link between data and the individual with whom the data is initially associated"
- Goal is to **mitigate privacy risks to individuals** while **supporting the secondar use of data** for various purposes
- HIPAA Privacy Rule
  1. **Expert Determination** - statistical/scientific principles; very small risk c re-identification
  2. **Safe Harbor** - removal of 18 types of identifiers
- State Law
  - Data that cannot reasonably be used to infer information about, or linked to, an identified or identifiable consumer

    PLUS
  - **Reasonable administrative measures** to prevent re-identification
  - **Public commitment** to maintaining de-identification
  - **Contractual obligations** on recipients not to reidentify



Practice Tip: you can't mix-and-match the Safe Harbor de-id process and the Expert Determination de-id process. PHI must be de-identified either by the Safe Harbor or the Expert Determination method. You can't combine the methods of both for a single resulting data set.

De-identification

Privacy+ Security Forum

- Some De-identification Practices
  - Removal
  - Masking
    - Irreversible Hashing
    - Encryption on a per-user/instance basis
  - k-anonymity (hiding in groups)
    - Generalization
    - Suppression
  - Randomization
  - Aggregate (Group Level) Processing
  - Differential Privacy - injecting noise
  - Combination Methods - this is data and company specific

De-identification

- De-identification is not a cure-all
  - HHS.gov: “Both methods, even when properly applied, yield de-identified data that retains some risk of identification. Although the risk is very small, it is not zero….”
  - Possibility that confidential information or trade secrets are leaked with de-identified dataset
  - Data Processing Impact Assessments are still very relevant
  - Other Privacy Enhancing Technologies could matter
    - Robust Access Controls
    - Federated Information Security
    - Regular Testing / Use-case Refinement
    - Role of Clean Rooms or Machine Learning

Health vs. Demographic Data

- **Market research** using **de-identified** information related to health can reveal statistical, population-level insights about health conditions
  - Basic insight: some health conditions predominantly affect men or women only (*e.g.*, prostate cancer or ovarian cancer, respectively)
  - Advanced insight: Some health conditions may be *more prevalent* along other (and potentially less intuitive) demographic factors such as a combination of age, gender, income or education level, geographic region, or other factors not directly related to a health condition
- Using these insights enables advertisers to define audiences **based on demographic characteristics only** with a higher likelihood of a health condition being relevant to that audience
- **Key concept:** An advertiser can know that a certain demographic group (e.g. men) has higher prevalence of a health condition and target advertisements based on that fact; but doing so does not reveal that any particular individual in that audience has the relevant health condition

Health vs. Demographic Data

Privacy+ Security Forum

- **Example:**
  - Take two demographic characteristics – age and sex
    - Incidence of prostate cancer among **men** that are **under 50 years old** is approximately 0.3%
    - Incidence of prostate cancer among **men** that are **50-59 years old** is approximately 2.0%
    - Source: https://www.medicalnewstoday.com/articles/age-range-for-prostate-cancer#prevalence-by-age
  - Advertisers seeking to share information about prostate cancer screening (e.g., a hospital group or insurance company) could increase the efficiency of those ads by nearly **10x** by targeting an audience believed to include only **men** that are **50-59 years old** compared to an audience of men under 50
  - Still, with only 2% prevalence in that segment, no individual's health status is obviously revealed or even reasonably inferred

Health vs. Demographic Data

- **Harder cases** – what if prevalence of a condition in an audience defined by demographics gets higher? What's an acceptable prevalence? 50%? 75%? 90%? Why?
  - For example, diabetes is highly prevalent in certain populations (especially older populations in certain geographic regions), even close to 50% prevalence for certain populations defined by a limited number demographic characteristics.
  - Adding additional layers of demographic data could result in segments with >50% prevalence – **is there a point at which an "inference" can no longer be avoided?**
  - Practices may diverge here, but adding noise can help achieve an appropriate prevalence percentage.

Health vs. Demographic Data

- NAI Demographic Health Advertising Best Practices provide a method to achieve efficiencies for health-related advertising without using sensitive personal information about a consumer's health
  - Source: https://thenai.org/press/the-nai-unveils-best-practices-for-health-advertising/
- Our standards focus on:
  - The use of demographic information that is not itself sensitive under state privacy laws
  - Avoiding the use of sensitive health information
  - Transparency into what demographic factors are used in audience creation
  - Minimum audience sizes

Collaboration between stakeholders

Privacy+ Security Forum

Collaboration between internal stakeholders is essential to creating effective, compliant, and ethical campaigns. Key aspects of collaboration:

- Cross-functional teams
  - Successful health-related advertising requires collaboration between various stakeholders, including marketing teams, healthcare professionals, legal advisors, data analysts, and compliance officers. Each group brings unique expertise that contributes to the development of accurate and effective campaigns
  - Leverage opportunities through collaboration
    - Joint initiatives for developing privacy-first advertising solutions
    - Creating a culture of privacy and trust within the organization
- Regulatory compliance
  - Establishing privacy policies and guidelines
  - Regular training and awareness programs
  - Implementation of data governance frameworks
  - Ensuring compliance with health regulations, such as HIPAA, is a critical aspect of health-related advertising. Legal and compliance teams work closely with marketing and data teams to ensure that all data used in advertising is handled in accordance with privacy laws and regulations.

Collaboration between stakeholders

Privacy+ Security Forum

- Ethical considerations
  - Legal and compliance teams play a critical role in reviewing advertising content and data usage to ensure adherence to ethical standards and regulations, such as HIPAA and FTC
- Monitoring and evaluation
  - Continuous monitoring and evaluation of advertising campaigns are essential to ensure they are effective and compliant
  - Stakeholders work together to assess the impact of campaigns and make necessary adjustments to improve outcomes
- Building trust with consumers
  - Transparent communication about data usage and privacy practices is essential to build trust with consumers
  - Engaging with healthcare professionals and patient advocacy groups can enhance credibility and ensure that advertising messages are responsible and ethical
- Feedback and Continuous Improvement
  - Encourage regular feedback from all stakeholders to identify areas for improvement
  - Implement changes based on feedback to enhance the effectiveness and compliance of advertising efforts

Key Takeaways

Privacy+ Security Forum

Key Takeaways

- Health-related advertising (and targeted advertising in general) is subject to a complicated and evolving set of rules
- Given the (potential) sensitivity of the underlying data, proper due diligence is important
- Exact compliance obligations depend on the rules that apply but certain best practices can be applicable throughout
- Data governance is still relevant (even to de-identified data)
- Critical to stay on top of new developments (e.g., DOJ Rule, Virginia reproductive health law, etc.)

Questions and Contact Information

Ali Jessani

ali.jessani@wilmerhale.com

Ben Chapman

ben@swoop.com

Robyn Eckerling

robyn.eckerling@tempus.com

Tony Ficarrotta

tony@networkadvertising.org