AMERICAN HEALTH LAW ASSOCIATION

HEALTH LAW WEEKLY

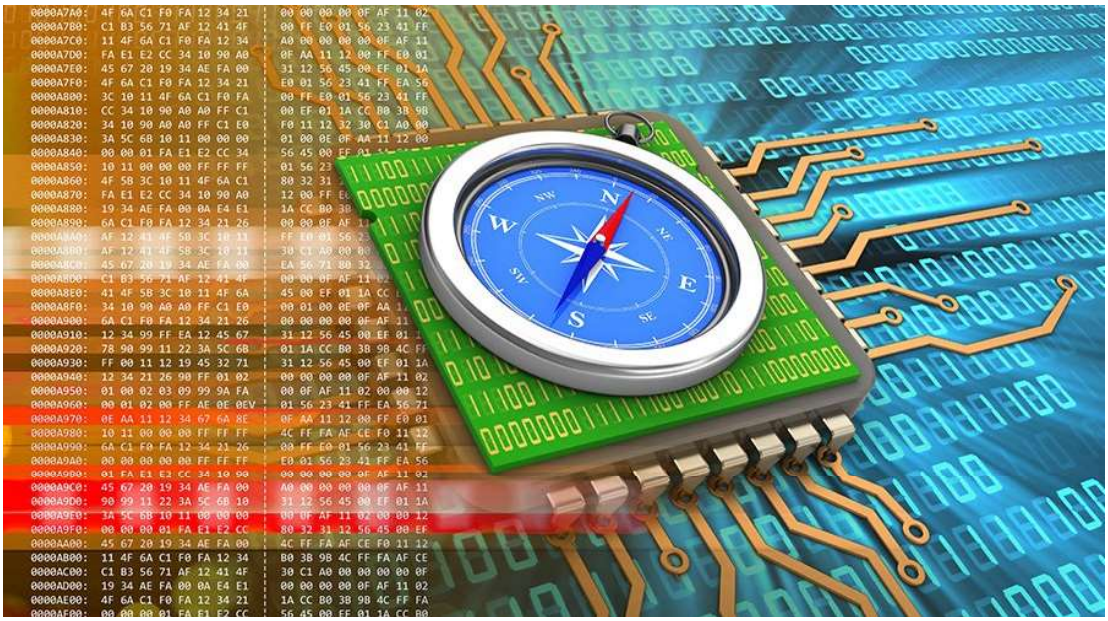
August 18, 2023

Advertising Analytics and Pixel Trackers in Health Care

Andrew Shaxted, FTI Consulting

Jamie Singer, FTI Consulting

Brian Boetig, FTI Consulting



By their nature, advertising analytics trackers and pixels collect information to support digital marketing and advertising processes across many industries, including health care. Depending on where the tracker is deployed and the configuration involved, advertising analytics trackers and pixels may collect and share personally identifiable information (PII), which may include identifiable health information and/or protected health information (PHI), posing a potential conflict with data protection requirements.

There are associated cyber threats and regulatory risk with collecting and sharing PII and PHI, especially in the health care industry, and unaware organizations are at risk of exposing sensitive patient information or facing noncompliance from inadequate protections. Valuable information to threat actors, like what operating system an individual is using, their IP address, or more concerningly, if they have entered PHI into the website, can be collected and accessed through pixel tracking.

These technologies are inexpensive (often free) and easy to deploy, yet require a level of technical sophistication to fully understand how they work. As such, governance and oversight is extremely challenging without the right support. Health care organizations that lack this governance but continue to make use of advertising analytics trackers face a wave of potential litigation and regulatory enforcement.

The plaintiff's bar has recently employed various state health record laws, state Unfair or Deceptive Acts Practices (UDAP) laws, federal and state wiretapping acts, and other legal theories (e.g., unjust enrichment, breach of fiduciary duty, negligence) to litigate the alleged improper use of advertising analytics trackers and pixels against health care and other organizations.

Further, the Department of Health and Human Services Office for Civil Rights issued guidance in December 2022 to address covered entity and business associate use of advertising analytics trackers and pixels.

For health care organizations and providers currently subject to litigation or regulatory information requests, there are three practical steps to take at the outset of such matters. These include:

1. Remediate after preservation. While it may be tempting to immediately remove problematic advertising trackers and pixels from a site upon receipt of a regulatory request for information or a complaint, doing so may damage an organization's ability to accurately collect the information needed to proffer a response. Instead, legal teams should work with IT and marketing functions to temporarily pause their use. Engaging an expert to perform a defensible collection and preservation of the sites at issue before further action is taken is essential.
2. Identify all relevant third-party digital marketing agencies, partners, and outside applications involved in the management and deployment of advertising analytics trackers. Issue appropriate litigation holds and take steps to preserve records, communications, and source code as appropriate.
3. Perform inventory of relevant third-party advertising analytics trackers and engage experts to support necessary collection, preservation, and analysis activities.

Further, health care organizations and providers risk class action, arbitration, and denied cyber insurance coverage if their pixel tracking services are mismanaged.

For organizations and providers seeking to limit regulatory, litigation, or reputational risk exposure in advance of a matter, the following five steps are important initial measures:

1. Coordinate across IT, marketing, and legal functions to perform a review and analysis of relevant websites and applications to identify potentially problematic activities.

2. Remediate or remove advertising analytics trackers that may violate data protection requirements, especially for health information, but be sure to track and manage versioning, so the related information is available if it becomes relevant to a matter later on.
3. Deploy technical and procedural controls to monitor changes in the environment and assess privacy risk, in advance of introducing new or modified advertising analytics and pixels onto the website.
4. Review existing contractual agreements that may exist between the organization and outside providers of analytics trackers. Several of the more ubiquitous providers have updated their terms to expressly state that their technology is not intended for sites where health information may exist. Take steps to review this material and to shift away from technologies that will not sign relevant contractual agreements and/or expressly state they should not be used for sites containing health information.
5. Plan for potential scenarios and public scrutiny. Privacy advocates leverage cybersecurity incidents, enforcement actions and broad consumer concerns to push for increased regulation and new laws, as well as to shame companies and scrutinize their behaviors and actions. To date, the use of trackers and advertising analytics tools have largely been covered by trade and national outlets, but local media outlets may also follow as companies make disclosures and reach settlements—increasing overall coverage and scrutiny. Corporate executives at health care organizations need to be prepared to communicate their organization's commitment to privacy, and be transparent about the collection and use of personal data.

Information valuable to threat actors, like what operating system an individual is using, their IP address, or more concerningly, if they have entered PHI into a website, can be collected and accessed through pixel tracking. Health care organizations that have not addressed these issues may be at risk of exposing sensitive patient information or facing noncompliance. Sound policy around the technologies must be developed and implemented. This will reduce complicated cybersecurity and regulatory concerns, while also protecting health data and sensitive information from exposure or theft.

About the Authors

Andrew Shaxted, a Managing Director within FTI Consulting's Technology segment, is an interdisciplinary technologist and lawyer specializing in privacy engineering, data and analytics, ad tech, digital forensics, and privacy governance.

A Managing Director and co-leader of Cybersecurity & Data Privacy Communications within FTI Consulting, **Jamie Singer** is a leading expert on cybersecurity crisis communications. Jamie has counseled Fortune 500 companies and public sector

organizations through some of the most high-profile and largest cybersecurity crises of the past decade.

Brian Boetig is a Senior Managing Director within FTI Consulting, with more than 33 years of national security, public safety and consulting experience, including as a United States diplomat, an Assistant Director at the Federal Bureau of Investigation, and a Director at the National Cyber Center.