BRITT
LAW

Your AI & Data Privacy Expert

PART 5 OF 6-PART SERIES

TRACKING TECHNOLOGIES FOR HIPAA-COVERED ENTITIES & OTHERS

THIS IS THE FIFTH OF A SIX-PART SERIES of commentaries on data management, authored by Steve Britt, managing partner of Britt Law LLC. These commentaries review the new laws and regulations relating to data privacy and artificial intelligence.

Steve is a deeply experienced **corporate and technology attorney** with world-class cyber, data privacy & artificial intelligence expertise, including three international data certifications. He also has extensive experience with software licensing, cloud, SaaS and data hosting. He practiced law in Washington, D.C. and Virginia prior to establishing Britt Law in Charleston, South Carolina. Steve formed Britt Law to leverage his data management experience and to offer a wider range of legal services with flexible fee arrangements. This includes fractional general counsel and fractional data protection engagements.

PART 5

INTRODUCTION

On March 18, 2024, the HHS Office of Civil Rights (OCR) issued a bulletin about the use of online tracking technologies by HIPAA-regulated entities resulting in the disclosure of protected health information (PHI). Tracking technology is a script, code or pixel embedded in a website or mobile app that gathers information on online visitors. It includes cookies, beacons, pixels, software development kits (SDKs) and session replay scripts.

These tools can have several benefits, but since they collect device and advertising IDs, they permit a third party to track users across unrelated websites. Often the owner of the site does not know that these tools are installed or, after requesting they be turned off, does not realize they are still operating in the background.

Information collected on a HIPAA-regulated site can constitute PHI if it relates to the user's past, present or future health, health care services or payment for health care. Under HHS guidelines, the determination of whether electronic health information constitutes PHI can turn on (i) whether the user had to authenticate (i.e., log in) into those webpages in order to access the data, and (ii) whether the user's purpose in accessing the webpage related to the user's past, present or future health care.

If PHI is deemed to have been accessed through the site, the covered entity must comply with the HIPAA Privacy Rule and the Security Rule. If the third-party recipient of the tracking data is a business associate, the covered entity must have entered into a business associate agreement with such entity.

If that were not complicated enough, **"consumer health data"** is a new category of health data under several new state data privacy laws. Those laws expressly exclude PHI as consumer health data because the business collecting this data is not a HIPAA-covered entity. The purpose of these new laws is to regulate health data collected by the thousands of commercial entities that are not regulated by HIPAA.

While not PHI, this information constitutes **"sensitive personal information"** under state data privacy laws, triggering a different set of compliance obligations.

For example, several states require that the business get affirmative consent from the consumer (i.e., opt-in) to the collection and processing of the user's sensitive information, while other states grant a right to opt-out of such processing.

That said, all state data privacy laws have a lot in common. For example, they require the following actions with regard to tracking data.

I. Provide reasonable security of such data.

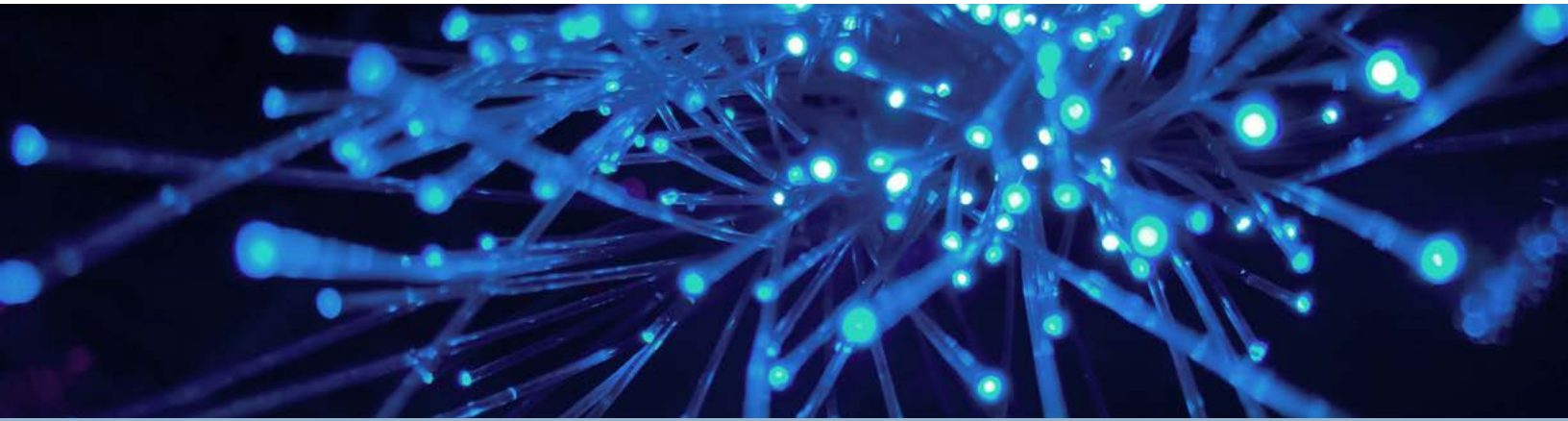
II. Execute a restrictive data protection agreement with the third-party recipient of the tracking data (rather than a business associate agreement for HIPAA-covered entities).

III. Comply with the FTC's Health Breach Notification Rule (HBNR) which can treat the unauthorized disclosure of this data as a data breach.

As proof of the legal risks of tracking, on July 30, 2024, the New York State Attorney General published "A Guide for Business - Website Privacy Controls". This guidance confirms that privacy controls and online tracking are subject to New York's consumer protection laws (even though New York does not yet have a data privacy statute).

This guidance resulted from a recent OAG investigation of e-commerce retailers that found that (i) privacy controls did not work as described, (ii) cookie notices were mislabeled, (iii) tools were misconfigured, and (iv) the effect of cookie opt-outs was misrepresented when tracking was not disabled. The OAG made clear that tracking is a continuing enforcement priority.

The use of tracking technology has triggered 50 class action lawsuits against hospitals and healthcare providers under the Video Privacy Protection Act, federal and state wiretapping laws and common law privacy rights. The FTC has fined GoodRx $1.5 million and BetterHelp $7.8 million. Patient class actions against Froedtert Health and Advocate Aurora Health have settled for up to $12.25 million.



KEY TAKEAWAYS

- All businesses should determine whether they are using tracking technologies. HIPAA-regulated entities should specifically determine if tracking is being used in association with health-related services, treatments or payments.
- Companies should have their own engineers review the code and operation of tracking technologies to see if cookies, pixels and beacons **"fire"** upon online visits and where the outputs are sent. Do not trust your vendor.
- Analyze the license terms for all software development kits (SDKs) incorporated into your site.
- If the business partner requires a business associate agreement, ensure that your BAA includes all of HHS' updated terms for such agreements.
- If your business is not regulated by HIPAA, determine what state and FTC rules apply to your collection and use of electronic health data and that you comply with such rules.
- Note that the Washington My Health My Data Act (WMHMDA) requires a separate consumer health data privacy notice, and remember that the WMHMDA contains a private cause of action.

There are several commercial software providers that conduct automated website and mobile app audits to avoid the unintended use of tracking technologies. Other software providers offer similar tools as part of a data management platform. We believe these are wise investments by any company that is at risk of these liabilities.

To learn more, contact Steve Britt at steve@brittlawllc.com.