Articles + Publications | May 4, 2023

Cookies and Online Tracking of Health Signals: An OCR Prescription for Potential Peril

WRITTEN BY

Ronald I. Raether Jr. | Erin S. Whaley | James Koenig | Brent T. Hoard | Laura Hamady | Robyn W. Lin

Online Tracking Technologies and HIPAA. In December 2022, the Department of Health and Human Services Office for Civil Rights (OCR) published a bulletin on the use of online tracking technologies (*e.g.,* cookies or web beacons) by entities regulated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Specifically, the OCR noted:

- In the course of gathering data, these online tracking technologies may collect protected health information (PHI); and
- The collection or analysis of the data may involve unauthorized disclosures of PHI to third-party tracking technology vendors or other related third-party vendors.

Most importantly, the OCR indicated that individually identifiable health information (IIHI) collected on a regulated entity's (*i.e.,* a covered entity's or business associate's) website or mobile app "generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."

- The OCR further explains that "tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider."

Five Steps You Can Take to Avoid HIPAA Tracking Issues. If you (1) use third-party tracking technologies on your website and/or apps; and (2) are a regulated entity (*i.e.,* a covered entity or business associate), then you need a practical approach to mitigate against unauthorized disclosures. Below find five steps you can take to avoid potential noncompliance issues under HIPAA:

1. **Prepare an inventory of cookies and tracking technologies.** Establish your baseline using tracking technology detection tools and interviews with IT and marketing.

2. **Determine internal uses.** Is the data collected and/or retained in aggregated or de-identified form (*e.g.*, to improve the website)? Is the data used for retargeting or other marketing purposes? What internal functional groups access and/or use the data?

3. **Establish the scope of third-party disclosures.** Are there contractual limitations/controls in place with the technology vendor? Are there disclosures of the data to any additional third parties (*e.g.*, secondary uses, such as AI/ML or other analytics)?

4. **Amend existing agreements/templates.** Amend existing vendor agreements with business associate agreements, as needed. Include a restriction on any data uses beyond delivering services (applicable to the business associate/vendor and any other sub-business associate service providers).

5. **Add a checkpoint in your vendor contracting and PIA processes.** Avoid future surprises by incorporating a tracking technology checkpoint in your procurement or contracting process and/or PIA workflow.

Questions. To learn more about the impact on your company and product pipeline, please contact Jim Koenig, Brent Hoard, Erin Whaley, Marc Loewenthal, Robyn Lin, or any member of our Privacy + Cyber team.

RELATED INDUSTRIES + PRACTICES

- Health Care + Life Sciences
- Privacy + Cyber