DORSEY
DORSEY+WHITNEY LLP

# Tracking Online User Activity: HIPAA and Other Legal Risks

*March 15, 2023 – Dorsey Health Law*
by Hannah McCallum and Ross C. D'Emanuele

The use of tracking technologies on websites and mobile applications (e.g., cookies) has become largely ubiquitous in our technology-driven world. Health care providers and organizations, for example, may use tracking technologies to identify their patients' care needs and improve patient experience.

As the use of tracking technologies burgeons, so do concerns from individuals about how to protect their personal information. Understandably so, as this technology comes with significant risks if collected information ends up in the wrong hands. Further, because of the sensitivity of the information involved, entities that handle Protected Health Information ("PHI") and are regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") must be particularly cautious when using tracking technologies.

On December 1, 2022, the Office of Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS"), which is responsible for enforcing HIPAA, issued a Bulletin addressing the use of tracking technologies by regulated entities, including Covered Entities and Business Associates, as defined by HIPAA.[1] The Bulletin does *not* create new obligations for HIPAA-regulated entities, and seeks only to clarify current HIPAA obligations as it relates to the use of tracking technologies, specifically, when a third-party vendor is utilized.

**What is a Tracking Technology?**

A tracking technology is a "script or code" on a website or mobile application ("app") that collects information about users as they interact with the website or application.[2] The information gathered is analyzed and used to

## Related People

- Hannah McCallum
- Ross C. D'Emanuele

## Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

"create insights about users' online activities", and even their personal characteristics, wants or needs.[3] Tracking technologies include mechanisms such as cookies, pixels, web beacons, and embedded tracking codes in apps and devices. One such example is the Facebook pixel by Meta, which website owners can embed into their website to track site visits and user activity on the website.[4]

**How is HIPAA Implicated?**

HIPAA-regulated entities are required to safeguard PHI, which includes protecting it from impermissible disclosures. When regulated entities utilize third-party vendors to track the activity of website or app users, information is collected through tracking technologies placed on the website or app, which is then sent to that vendor to perform data analytics. If the collected information includes PHI, it is protected by HIPAA, and the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") apply.[5]

The rule for what qualifies as PHI in this context is much broader than one might think. Sometimes it is apparent: a patient portal that a patient must log in to almost certainly has access to PHI, such as the person's medical or billing information.

**However**, even an unauthenticated webpage that does not require a login, such as a health care provider's public website, may provide a tracking technology vendor access to PHI. For example, tracking technologies might collect identifying information, such as an individual's email address or IP address. If that person then begins searching for a provider or information on a particular medical condition, which is also tracked and sent to the vendor, the regulated entity is now disclosing PHI to the vendor.[6]

Likewise, mobile apps may collect information such as health and billing information, as well as information about the user's device (fingerprints, network location, etc.). This, too, is PHI, and any disclosure to the vendor must comply with HIPAA.

**Purported Class Action Lawsuits**

In recent months, several health plans and hospital systems have been the target of purported class action lawsuits from private plaintiffs alleging that the defendants utilized tracking technology vendors and unlawfully disclosed PHI without individual consent. Because there is no private right of action under the HIPAA Rules, these lawsuits do not bring HIPAA claims. But they appear to use alleged HIPAA Rule violations as a basis for claims under the Electronic Communication Privacy Act of 1986, the Computer Fraud and Abuse Act, and state law common law privacy claims. Accordingly, this is not merely a technical HIPAA matter, and can result in real consequences.

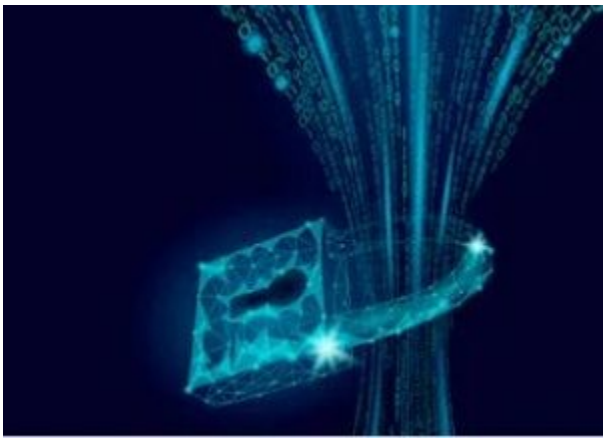
**What Should Regulated Entities Do to Comply with HIPAA When Using Tracking Technology Vendors?**

- Make sure a Business Associate Agreement ("BAA") is in place. A tracking technology vendor is a Business Associate when it creates, receives, maintains, or transmits PHI on behalf of a Covered Entity.[7] Further, disclosures to the vendor must be permitted by the HIPAA privacy rule, and only the minimum necessary PHI

for the applicable purpose may be disclosed.

- If a BAA is not practicable or sufficient (e.g., there is no applicable permitted disclosure under the HIPAA privacy rule), the regulated entity must obtain individuals' HIPAA-compliant authorization ***before*** any disclosure to the vendor occurs.[8] It is worth noting here certain mechanisms that do **not** qualify as HIPAA-compliant authorization:
  - Privacy policy or terms of use. While a regulated entity may disclose the use of tracking technology here, that is insufficient to permit a disclosure of PHI that requires an individual's authorization under the HIPAA privacy rule.
  - Website banners asking individuals to accept or reject tracking technologies, such as cookies.
  - A tracking technology vendor that promises to de-identify PHI before using information it receives or promises not to save PHI, because disclosure has already occurred at that point.

- Apply administrative, physical and technical safeguards to electronic PHI, as required under the Security Rule (e.g., encrypt PHI sent to the vendor), and consider and address tracking technologies when performing risk assessments.
- Notify individuals, the Secretary, and the media as required if a breach occurs.



**Final Thoughts**

HIPAA-regulated entities that utilize tracking technologies, and in particular, tracking technology vendors, must remain vigilant as to how PHI may be collected on various platforms. In particular, be aware that even a public, unauthenticated webpage could result in disclosure of PHI due to identity- or device-tracking pixels.

When using a tracking technology vendor, a BAA must be in place, and the purpose of the disclosure must be permitted under the HIPAA Rules. Failure to do could result in impermissible disclosure of PHI, constituting a violation of the HIPAA Rules. The practice could also attract claims from private plaintiffs under various statutory and common law theories.

Be proactive in addressing this potential gap in your privacy program; do not wait until the problem finds you.

[1] 45 CFR § 160.103.

[2] Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, Dep't of Health & Human Services (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html - ftn8.

[3] *Id.*

[4] *See* https://www.facebook.com/gpa/blog/the-facebook-pixel.

[5] *See* 45 CFR parts 160 and 164.

[6] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html - ftn8.

[7] *Id.*

[8] 45 CFR § 164.508(b).