Proceed with Caution: Online Tracking Technologies Pose HIPAA Compliance Risks

March 2, 2023

On December 1, 2022, the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued guidance[1] to covered entities[2] and their business associates (collectively, "regulated entities") concerning online tracking technology. The use of tracking technologies on websites and mobile applications has long been a commonplace aspect of the online ecosystem, providing companies with valuable insights into user behaviors as well as opportunities to enhance user experiences. However, healthcare entities' use of tracking technologies, such as cookies, web beacons and pixels, has recently come under fire: a litany of class-action lawsuits alleging improper disclosure of patient information has been filed against major health systems and hospitals. For example, in 2022, Mass General Brigham and the Dana-Farber Cancer Institute reached an $18.4 million "cookies without consent" settlement to resolve allegations that tracking tools on the institutions' informational websites transferred and sold users' information without their prior written consent in violation of state privacy and consumer protection laws.[3]

In the wake of such unlawful tracking suits, OCR issued broad-reaching guidance indicating that certain information collected from websites and applications via online tracking technology may implicate the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Although HIPAA does not itself provide a private right of action, it is commonly cited in consumer actions that allege improper use and disclosure of sensitive patient data. Indeed, OCR's guidance appears to have emboldened additional class actions by plaintiffs seeking redress for alleged privacy violations: complaints filed this year against Cedars-Sinai Medical Center and Christ Hospital expressly cite the OCR bulletin.

---

1 OCR's bulletin, titled "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," can be found here.

2 HIPAA covered entities include (1) health plans, (2) health care clearinghouses and (3) health care providers who conduct certain financial and administrative transactions electronically.

3 Mass General Brigham, Dana-Farber to pay $18.4M settlement over privacy allegations, available at: https://www.bizjournals.com/boston/news/2022/01/06/mass-general-brigham-dana-farber-to-pay-184m-se.html.

Below, we provide a brief overview of OCR's guidance as well as preliminary steps regulated entities can take to assess compliance risk.

KEY TAKEAWAYS FROM THE OCR BULLETIN

- **Because regulated entities' user-authenticated webpages[4] generally contain protected health information ("PHI"), regulated entities must enter into a business associate agreement ("BAA") with a vendor in order to utilize tracking services.** OCR guidance states that user-authenticated webpages (*e.g.*, patient portals) often contain PHI such as medical record numbers, appointment dates, diagnosis and billing information and other identifying information provided by a user. Any disclosure is thus regulated by HIPAA and a tracking technology vendor is considered a regulated entity and, therefore, must be bound by a BAA before receiving PHI.

- **Utilizing tracking technologies may require a BAA even where there is no patient relationship between the user and the regulated entity.** OCR guidance states that unauthenticated webpages[5] are generally not regulated by HIPAA. However, OCR takes the expansive view that information tracked from an unauthenticated site shall nonetheless be considered PHI if: (i) it is collected by a regulated entity; (ii) it relates to an individual's past, present or future healthcare or payment for healthcare—*regardless* of whether there is an existing relationship with such regulated entity—and (iii) it can be linked to a specific individual. In other words, tracking information collected by a regulated entity on an unauthenticated webpage from an individual who is not an existing patient of such entity is broadly *presumed* by OCR to relate to such individual's past, present or future healthcare or payment for healthcare.

- **Mobile applications ("apps") offered by regulated entities are subject to HIPAA; apps provided from other entities may be governed by other privacy laws.** OCR's guidance recognizes that the provision of healthcare often involves the use of apps, which allow individuals to access and manage their health information and to pay bills. These apps collect a wide variety of information that could qualify as PHI, such as fingerprints, network or geographic location and the user's device ID. Thus, a

---

[4] A "user-authenticated webpage" verifies the identity of a user attempting to gain access to the webpage, *i.e.,* requires a user to log in before access is granted.

[5] An "unauthenticated webpage" does not require a user to log in before accessing the contents of the webpage. OCR's guidance states that the unauthenticated webpage of a regulated entity often contains general information about the regulated entity, such as its location.

regulated entity that collects such information and discloses it to a tracking technology vendor, the app vendor or a third party, must comply with HIPAA. Notably, HIPAA's restrictions only extend to apps offered *by or on behalf of* a regulated entity, not to apps offered by non-regulated entities. Nonetheless, OCR warns that other state and federal privacy laws may apply to the use and disclosure of such information.

ACTION ITEMS FOR REGULATED ENTITIES

OCR's guidance has far-reaching consequences for covered entities as well as business associates, including heightened risk of litigation. As noted above, complaints filed this year against Cedars-Sinai Medical Center and Christ Hospital expressly cite the OCR bulletin, including the agency's description of individually-identifiable tracking information as "highly sensitive,"[6] and its bold proclamation that a regulated entity's implementation of third-party tracking technology absent notice to, and written authorization from, users constitutes a HIPAA violation.[7] In light of these developments, regulated entities should examine whether their current or future tracking technology vendors have or will receive PHI and, if so, should consider the following action items:

- tracking technology vendors with access to PHI must enter into a BAA that specifies the permitted and required uses and disclosures of PHI and provides that the vendor will appropriately safeguard any PHI it receives and report security incidents to the regulated entity;

- absent a BAA, a healthcare entity may not disclose PHI to a vendor without a patient's authorization[8] and

- regulated entities should appropriately staff compliance teams to address breach notifications requirements, as required by HHS in the event of impermissible disclosure of PHI through the use of tracking technology.

Furthermore, even where online tracking technologies collect information that is not considered PHI, regulated entities should consider whether other privacy laws apply,

---

6 *See* Doe v. Cedars-Sinai Health System and Cedars-Sinai Medical Center, Case: 2:23-cv-00870 at ¶ 104.

7 *See* Doe v. The Christ Hospital, Case: 1:23-cv-00031-DRC at ¶ 88.

8 OCR also clarified in its Guidance that it is impermissible to obtain "authorization" for the disclosure of PHI through a standard privacy policy, notice or terms and conditions as opposed to explicit positive permission from the patient.

such as the Federal Trade Commission's Health Breach Notification Rule and the California Consumer Privacy Act.

* * *

We will continue to monitor OCR's HIPAA enforcement patterns for any updates or changes. Please do not hesitate to contact us with any questions.

NEW YORK

Andrew L. Bab
albab@debevoise.com

Jennifer L. Chu
jlchu@debevoise.com

Mark P. Goodman
mpgoodman@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Kevin Rinker
karinker@debevoise.com

Hannah R. Levine
hrlevine@debevoise.com

SAN FRANCISCO

Michael L. Cederblom
Law Clerk
mlcederblom@debevoise.com

Kim T. Le
kle@debevoise.com