BCLP. Client Intelligent

Insights

NEW HHS GUIDANCE ON COOKIES

May 30, 2024

On March 18, 2024, the Office of Civil Rights ("OCR") within the Department of Health and Human Services ("HHS") updated prior guidance concerning the use of online tracking technologies, including cookies, by Covered Entities and Business Associates (prior guidance available here).

The new guidance is largely a revisitation and clarification of prior guidance by OCR, which applied very broadly to common marketing and analytic practices in the industry. The prior guidance — especially the breadth of what qualified as PHI and as such was regulated by HIPAA — was quite controversial, triggering a lawsuit from the American Hospital Association and certain other plaintiffs challenging its validity on various grounds.

The new guidance can be read as a slight revision of HHS's original position on the issue. For example, HHS concedes that in most cases a non-user authenticated visit to a website, even one addressing specific disease states, will not constitute PHI, stating ". . . the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI [individually identifiable health information] if the visit to the webpage is not related to an individual's past, present or future health, health care, or payment of health care."

The guidance provides examples of situations in which such tracking would not constitute PHI—examples such as a visit to a hospital homepage to check hours, or a visit by a researcher to check the availability of specialist appointments. But not all the guidance is helpful in this regard. One example is innocuous enough (even trivial)—the case where a user inputs actual text indicating a disease state and/or provides a diagnosis for analysis; but another example—the case where a user visits a website listing oncology services "to seek a second opinion" without more—is nearly indistinguishable from the researcher example above. Yet the second opinion example also is PHI according to the guidance. In both cases the user visits a webpage to check the availability of an appointment, one is for market research purposes, the other is because an appointment is desired. How is the Covered Entity to distinguish between the two without more data?[1]

The stakes are high. Mere reliance on consent for transmission of PHI to third parties is likely under the guidance to violate HIPAA privacy obligations if the transmission is not supported (or

supportable) by a BAA or a permissible disclosure under the Privacy Rule. Without these legal grounds, a patient authorization is technically required for the disclosure, but it is very challenging (or likely impossible) to obtain a HIPAA compliant authorization in most circumstances (e.g., *before* cookies drop on a consumer's terminal).

Concerning authenticated visits, the new guidance cedes little ground, stating "[t]racking technologies on a regulated entity's user-authenticated webpages generally have access to PHI." Likewise, data collected by mobile applications will generally be considered PHI. This means that when users are logged in to mobile applications operated by a Covered Entity or Business Associate or have logged in to a website operated by a Covered Entity or Business Associate and have communicated IIHI (such as by searching for treatment options), this data will qualify as PHI.

Finally, the guidance addresses compliance issues. For example:

- Where a tracking technology is supported by a vendor, and that vendor meets the definition of a "Business Associate," a Business Associate Agreement should be executed. The guidance anticipates that some entities that qualify as Business Associates may not be willing to execute BAAs, in which case it suggests utilizing an intermediary to de-identify the data in question.
- Of course, not all transmissions are to Business Associates, and indeed not all processing or operations are Business Associate functions. In those instances, an authorization likely is required.

In short, while the new guidance appears to offer more leeway concerning unauthenticated web pages, OCR has largely stuck to their original position concerning authenticated web pages and mobile devices. Covered Entities and Business Associates should actively monitor their digital properties and consult with counsel concerning whether and how cookies, SDKs, and pixels should be deployed.

FOOTNOTE

[1] It should be noted that the "second opinion" example is qualified such that the data is PHI solely "to the extent that the information is both identifiable and related to the individual's health or future care" but it is unclear what this means as a practical matter.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564
