ACA, HIPAA AND FEDERAL HEALTH BENEFIT MANDATES: PRACTICAL Q&A

The Affordable Care Act (ACA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other federal health benefit mandates (e.g., the Mental Health Parity Act, the Newborns and Mothers Health Protection Act, and the Women's Health and Cancer Rights Act) dramatically impact the administration of self-insured health plans. This monthly column provides practical answers to administration questions and current guidance on ACA, HIPAA and other federal benefit mandates.

Attorneys John R. Hickman, Ashley Gillihan, Carolyn Smith, Ken Johnson, Amy Heppner, and Laurie Kirkwood provide the answers in this column. Mr. Hickman is partner in charge of the Health Benefits Practice with Alston & Bird, LLP, an Atlanta, New York, Los Angeles, Charlotte, Dallas and Washington, D.C. law firm. Ashley, Carolyn, Ken, Amy, and Laurie are senior members in the Health Benefits Practice. Answers are provided as general guidance on the subjects covered in the question and are not provided as legal advice to the questioner's situation. Any legal issues should be reviewed by your legal counsel to apply the law to the particular facts of your situation. Readers are encouraged to send questions by E-MAIL to Mr. Hickman at john.hickman@alston.com.

STRANGER DANGER: AVOIDING THE PITFALLS OF HIPAA AND ONLINE TRACKING TECHNOLOGIES

On December 1, 2022, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services ("HHS") issued the bulletin "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" ("Bulletin").

This Bulletin sets forth OCR's views as to the obligations of entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) ("Regulated Entities") when using online third-party tracking technologies (e.g., cookies, web beacons, session replay scripts, and fingerprinting scripts) through websites or mobile apps. As OCR explains, online tracking technologies collect and analyze information about how users interact with a Regulated Entity's websites or mobile apps.

According to OCR, these tracking technologies send information directly to the third parties who developed them and may continue to track users even after the user navigates to other websites, and therefore potential HIPAA concerns can arise.

The Bulletin expresses OCR's view of how HIPAA Rules apply to information disclosed to third-party tracking technology vendors ("TT Vendors") from a Regulated Entity's website or mobile app.

Of particular interest is how information collected from a Regulated Entity's publicly accessible webpage could be, in OCR's view, considered protected health information ("PHI", or "ePHI", if disclosed electronically), even if a user has no current relationship with the Regulated Entity, and even if the user does not actively provide any specific health care information.

For example, according to OCR, if a user visits a Regulated Entity's public webpage to search for available appointments with a provider and the TT Vendor collects information about the user's activity, along with the user's IP address or email address, the information may be PHI.

The analysis is not formally explained but seems to hinge on whether the information indicates that the person has received or will receive health care services or benefits from the Regulated Entity. The Bulletin does not address the scenario where an individual (such as a spouse, parent or guardian) uses a Regulated Entity's public webpage to search for potential providers on behalf of another person (the potential patient).

OCR's broad view of the type of information that constitutes PHI will present challenges for Regulated Entities. In the Bulletin, OCR instructs Regulated Entities to review disclosures of PHI made to TT Vendors on the Regulated Entity's user-authenticated webpages (i.e., sites that require a login or other credentials to access), unauthenticated webpages (sites accessible by the general public without a login), and mobile apps to confirm that the disclosures are permissible under HIPAA's Privacy Rule, and that ePHI is protected and secured consistent with the HIPAA Security Rule.

According to OCR, if the disclosure is made for a HIPAA-permitted purpose, the Regulated Entity needs to determine if the TT Vendor is a "business associate" under HIPAA. If so, the Bulletin expects the Regulated Entity to convince the TT Vendor to enter into a HIPAA business associate agreement ("BAA"), which may also be challenging.

If the disclosure is made for a purpose other than treatment, payment, or healthcare operations (or any other purpose permitted under HIPAA's Privacy Rule), or

if a TT Vendor is not a HIPAA business associate, then OCR's Bulletin states a HIPAA-compliant authorization would be required.

In OCR's view, such failure to obtain a HIPAA authorization may trigger HIPAA's breach notification requirements. The Bulletin makes it clear that website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization.

A Regulated Entity's failure to comply with the HIPAA Rules may result in a civil money penalty. Furthermore, OCR states that use of these tracking technologies needs to be addressed in the Regulated Entity's HIPAA Risk Analysis and Risk Management process under the HIPAA Security Rule.

The Bulletin does not specifically address potential scenarios involving an exception to the definition of a "breach," a low-risk determination under HIPAA's breach notification rules, and/or PHI which has been sufficiently encrypted such that it is not "Unsecured PHI."

TRACKING ON USER-AUTHENTICATED WEBPAGES

OCR uses the phrase "user-authenticated webpage" to mean that a person has to log in using a unique ID and password or some other credential. The Bulletin presumes that information on webpages offered by a Regulated Entity will likely always be PHI, and therefore HIPAA privacy and security rules will always apply.

OCR's Bulletin requires Regulated Entities to evaluate whether the information disclosed to a third-party TT Vendor is disclosed for a permissible purpose under the HIPAA Privacy Rule and to confirm that any disclosure of electronic PHI adheres to the HIPAA Security Rule. Additionally, under the Bulletin's parameters, if the third-party TT Vendor creates, receives, maintains, or transmits PHI on behalf of the Regulated Entity, then the vendor would be a HIPAA business associate, and a BAA needs to be in place prior to any disclosure of PHI.

TRACKING ON UNAUTHENTICATED WEBPAGES

OCR uses the phrase "unauthenticated webpage" to mean that the page is accessible to the general public and no login is required. This webpage could

PAYMENTS DONE RIGHT

Saving our customers over $1B a year.

An end-to-end solution tailored to your needs:

CONNECTION
to over 1M+ vendors

COMPLIANCE
across HIPAA, PCI, OFAC, and IRS 1099 reporting

EFFICIENCY
that streamlines and reconciles through one system

EASE OF USE
with quick deployment and training for your team

ECHO®
Payments *Simplified*

Contact us to learn more.
echohealthinc.com | 440.835.3511

be the Regulated Entity's general information page where the entity posts its location, services, and policies and procedures.

OCR's Bulletin assumes that tracking technologies on these types of general information pages generally have no access to PHI. However, the Bulletin describes, by way of example, the types of unauthenticated webpages that could provide an opportunity (in OCR's view) for PHI to be disclosed to third party TT Vendors, such as login pages, registration pages, webpages with search functionalities, and webpages that address specific symptoms or health conditions.

- **Login/registration page**. Usually anyone can access a Regulated Entity's login page, such as a patient portal, or a registration page. If a person enters credential information on a login webpage or enters registration information (e.g., name, email address) on a registration page, OCR's Bulletin views this as PHI.
- **Webpages that address specific symptoms or health conditions**. Regulated Entities may allow a user to search for information about a specific symptom or health condition, or search for a doctor or available appointment on its public website. OCR's Bulletin takes the position that PHI may be disclosed if this information, along with IP address or email address, is disclosed to the TT Vendor.

The Bulletin flags these webpages as areas that require further inquiry but does not provide a clear framework for analyzing when PHI is created. The relevant inquiry seems to be at the nexus of the tracking technology's ability to collect, at a minimum, the user's IP address, geographic location or email address (assuming the individual is using their personal computer or mobile device) and whether the nature of the user's activity on the webpage is "indicative that the individual has received or will receive health care services or benefits from the covered entity."

The right solution

Self-funded health plan administration

The speed of change in the health care industry is expanding the definition of health care and redefining roles for traditional players. New and emerging technologies led by single point solution vendors, rising health care costs, regulation, and non-traditional market entrants have many payers and health systems evaluating their options.

At AmeriHealth Administrators, we have a proven history of working with employer and payer clients to address their challenges and have the vision, technology, and people to meet the needs of our customers and partners.

Let us build the right solution for you.

Email us at sales@ahatpa.com

1599500 11-21

The Bulletin appears to assume that the individual who is using the login/registration page or webpage is the patient himself or herself and not someone (such as a parent, spouse or guardian) who might be searching for information on behalf of another person (the actual/future patient).

TRACKING WITHIN MOBILE APPS

Some Regulated Entities offer mobile apps that provide services to users, such as helping to manage a user's health information or pay bills. The Bulletin states that this type of information, when coupled with identifiable information such as fingerprints (i.e., device name, type, operating system version, and IP address), network location, geolocation, device ID, or advertising ID, is PHI. According to OCR, Regulated Entities also need to be aware of disclosures to the mobile app vendor or any other third party who receives such information.

OCR expressed concern regarding disclosures related to women's reproductive health, such as mobile apps offered by Regulated Entities that people may use to track their menstrual cycle, body temperature, or contraceptive prescription information.

HIPAA COMPLIANCE STEPS WHEN USING TRACKING TECHNOLOGIES

OCR's Bulletin outlines and clarifies some compliance requirements for Regulated Entities using third-party tracking technologies. Essentially, according to OCR, disclosures of PHI to third party TT Vendors are to be treated like any other third-party disclosure, requiring an analysis of permissible HIPAA purposes, a BAA, and HIPAA-compliant authorizations. The Bulletin lists the following HIPAA obligations for Regulated Entities using tracking technologies:

- Ensuring that all disclosures of PHI to TT Vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.

- Establishing a BAA with a TT Vendor that meets the definition of a "business associate." The BAA must specify the TT Vendor's permitted and required uses and disclosures of PHI and provide that the TT Vendor will safeguard the PHI and report any security incidents, including breaches of unsecured PHI, to the Regulated Entity, among other requirements. If a Regulated Entity does not want to create a business associate relationship with these TT Vendors, or the chosen TT Vendor will not provide written satisfactory assurances in the form of a BAA that it will appropriately safeguard PHI, then the Regulated Entity cannot disclose PHI to the TT Vendor without individuals' HIPAA-compliant authorizations.

- Addressing the use of tracking technologies in the Regulated Entity's Risk Analysis and Risk Management processes, as well as implementing other administrative, physical, and technical safeguards in accordance with the Security Rule (e.g., encrypting ePHI that is transmitted to the TT Vendor; enabling and using appropriate authentication, access, encryption, and audit controls when accessing ePHI maintained in the TT Vendor's infrastructure) to protect the ePHI.

- Providing breach notification to affected individuals, the Secretary of HHS, and the media (when applicable) of an impermissible disclosure of PHI to a TT Vendor that compromises the security or privacy of PHI when there is no Privacy Rule requirement or permission to disclose PHI and there is no BAA with the TT Vendor. In such instances, OCR takes the position that there is a presumption that there has

been a breach of unsecured PHI unless the Regulated Entity can demonstrate that there is a low probability that the PHI has been compromised.

OCR's Bulletin characterizes the following attempts at compliance to be insufficient:

- Regulated Entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does not permit disclosures of PHI to a TT Vendor based solely on a Regulated Entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated Entities must ensure that all TT Vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.

- If there is not an applicable Privacy Rule permission or if the TT Vendor is not a business associate of the Regulated Entity, then the individuals' HIPAA-compliant authorizations are required before the PHI is disclosed to the TT Vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization.

- Further, OCR views it as insufficient for a TT Vendor to agree to remove PHI from the information it receives or de-identify the PHI before the TT Vendor saves the information. The Bulletin states that any disclosure of PHI to the TT Vendor without individuals' HIPAA-compliant authorizations requires the TT Vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure.

- Signing an agreement containing the elements of a BAA does not make a TT Vendor a business associate if the TT Vendor does not meet the business associate definition.

In the Bulletin, OCR does not apply the HIPAA Rules to information that users voluntarily download or enter into mobile apps that are not developed or offered by or on behalf of Regulated Entities, even if the individual obtained that information from their medical record created by a Regulated Entity.

Although HIPAA does not cover these situations, OCR states that other federal laws may apply. While this is not included in the Bulletin, Regulated Entities and non-Regulated Entities should also be aware the disclosure of non-PHI health and medical information to TT Vendors and other digital advertising and analytics providers, and the use of non-PHI health and medical information for targeted advertising, is regulated under Section 5 of the FTC Act and state privacy laws, such as the California Consumer Privacy Act and the Virginia Consumer Data Protection Act.

Although bulletins do not have the force and effect of law, OCR does enforce and administer HIPAA Rules and is responsible for investigating breach reports and complaints. The Bulletin represents OCR's current view of how HIPAA Rules apply to information disclosed to TT Vendors and provides insights as to OCR's likely enforcement positions. ■