Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities[1] and business associates[2] ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[3] OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities' noncompliance with the HIPAA Rules. A regulated entity's failure to comply with the HIPAA Rules may result in a civil money penalty.[4]

Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations.[5] The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI).[6] Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.[7] **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures[8] of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[9]

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule[10] but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.

This Bulletin provides a general overview of how the HIPAA Rules apply to regulated entities' use of tracking technologies. This Bulletin addresses:

- What is a tracking technology?
- How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
    - Tracking on user-authenticated webpages[11]
    - Tracking on unauthenticated webpages[12]
    - Tracking within mobile apps[13]
    - HIPAA compliance obligations for regulated entities when using tracking technologies

What is a tracking technology?

Generally, a tracking technology is a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app ("website owner" or "mobile app owner"), or third parties, to create insights about users' online activities. Such insights could be used in beneficial ways to help improve care or the patient experience. However, this tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment.

Tracking technologies collect information and track users in various ways,[14] many of which are not apparent to the website or mobile app user. Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts[15] to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user's mobile device-related information. For example, mobile apps may use a unique identifier from the app user's mobile device, such as a device ID[16] or advertising ID.[17] These unique identifiers, along with any other information collected by the app, enable the mobile app owner or vendor or any other third party who receives such information to create individual profiles about each app user.[18]

Website or mobile app owners may use tracking technologies developed internally or those developed by third parties. Generally, tracking technologies developed by third parties (*e.g.*, tracking technology vendors) send information directly to the third parties who developed such technologies and may continue to track users and gather information about them even after they navigate away from the original website to other websites. This Bulletin focuses on regulated entities' obligations when using third party tracking technologies.

How do the HIPAA Rules apply to regulated entities' use of tracking technologies?

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI)[19] that the individual provides when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.[20] All such IIHI collected on a regulated entity'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.[21] This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[22]

Tracking on user-authenticated webpages

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI. Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI)[23] collected through its website is protected and secured in accordance with the HIPAA Security Rule.[24]

Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.*, health care operations[25]) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules.[26],[27] For example, if an individual makes an appointment through the website of a covered health clinic[28] for health services and that website uses third party tracking technologies, then the website

might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.

Tracking on unauthenticated webpages

Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, services they provide, or their policies and procedures. Tracking technologies on regulated entities' unauthenticated webpages generally do not have access to individuals' PHI; in this case, a regulated entity's use of such tracking technologies is not regulated by the HIPAA Rules. **However**, in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include:

- The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal, generally are unauthenticated because the individual did not provide credentials to be able to navigate to those webpages. However, if the individual enters credential information on that login webpage or enters registration information (*e.g.*, name, email address) on that registration page, such information is PHI.[29] Therefore, if tracking technologies on a regulated entity's patient portal login page or registration page collect an individual's login information or registration information, that information is PHI and is protected by the HIPAA Rules.
- 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. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

Tracking within mobile apps

Mobile apps[30] that regulated entities offer to individuals (*e.g.*, to help manage their health information, pay bills) collect a variety of information provided by the app user, including information typed or uploaded into the app, as well as information provided by the app user's device, such as fingerprints,[31] network location,

geolocation, device ID, or advertising ID. Such information collected by a regulated entity's mobile app is PHI, and thus the regulated entity must comply with the HIPAA Rules for any PHI that the mobile app uses or discloses, including any subsequent disclosures to the mobile app vendor, tracking technology vendor, or any other third party who receives such information. For example, the HIPAA Rules apply to any PHI collected by a covered health clinic through the clinic's mobile app used by patients to track health-related variables associated with pregnancy (*e.g.*, menstrual cycle, body temperature, contraceptive prescription information).

However, the HIPAA Rules do not protect the privacy and security of information that users voluntarily download or enter into mobile apps that are not developed or offered by or on behalf of regulated entities, regardless of where the information came from. For example, the HIPAA Rules do not apply to health information that an individual enters into a mobile app offered by an entity that is not regulated by HIPAA (even if the individual obtained that information from their medical record created by a regulated entity). In instances where the HIPAA Rules do not apply to such information, other law may apply. For instance, the Federal Trade Commission (FTC) Act and the FTC's Health Breach Notification Rule (HBNR) may apply in instances where a mobile health app impermissibly discloses a user's health information.[32]

HIPAA compliance obligations for regulated entities when using tracking technologies

Regulated entities are required to comply with the HIPAA Rules when using tracking technologies. Some examples of the HIPAA Privacy, Security, and Breach Notification requirements that regulated entities must meet when using tracking technologies with access to PHI include:

- Ensuring that all disclosures of PHI to tracking technology 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.[33]
    - 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.[34] However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology 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 tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.[35]
    - If there is not an applicable Privacy Rule permission or if the 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 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, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.
- Establishing a BAA with a tracking technology vendor that meets the definition of a "business associate."
    - A regulated entity should evaluate its relationship with a tracking technology vendor to determine whether such vendor meets the definition of a business associate and ensure that the disclosures made to such vendor are permitted by the Privacy Rule. A tracking technology vendor is a business associate if it meets the definition of a business associate, regardless of whether the required BAA is in place.[36] Moreover, signing an agreement containing the elements of a BAA does not make a tracking technology vendor a business associate if the tracking technology vendor does not meet the business associate definition.
    - The BAA must specify the vendor's permitted and required uses and disclosures of PHI and provide that the vendor will safeguard the PHI and report any security incidents, including breaches of unsecured PHI, to the regulated entity, among other requirements.[37]
    - If a regulated entity does not want to create a business associate relationship with these vendors, or the chosen tracking technology vendor will not provide written satisfactory assurances in the form of a BAA that it will appropriately safeguard PHI, then the entity cannot disclose PHI to the vendors without individuals' authorizations.
- Addressing the use of tracking technologies in the regulated entity's Risk Analysis and Risk Management processes,[38] 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 tracking technology vendor;[39] enabling and using appropriate authentication, access, encryption, and audit controls when accessing ePHI maintained in the tracking technology vendor's infrastructure)[40] to protect the ePHI.
- Providing breach notification[41] to affected individuals, the Secretary, and the media (when applicable) of an impermissible disclosure of PHI to a tracking technology 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 vendor. In such instances, 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.[42]

Endnotes:

[1] *See* 45 CFR 160.103 (definition of "Covered entity").

[2] *See* 45 CFR 160.103 (definition of "Business associate").

[3] *See* 45 CFR parts 160 and 164. *See also* OCR's Fact Sheet on Direct Liability of Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

[4] *See* 42 USC 1320d-5; *see also* 45 CFR part 160, subpart D; and 2019 Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, 84 FR 18151 (April 30, 2019). For more information on breach reporting, see also OCR's Guidance on the Breach Notification Rule, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[5] Health care operations include customer service, business planning and development, and business management or general administrative activities. *See* 45 CFR 164.501 (definition of "Health care operations"). This Bulletin does not address all potential purposes for which a regulated entity might use tracking technologies and the specific conditions that apply to uses and disclosures for those purposes. For example, uses and disclosures of PHI for purposes of research, such as research studies that involve the collection of PHI using tracking technologies, are not within the scope of this bulletin; those uses and disclosures are subject to the requirements of the Privacy Rule's research provisions at 45 CFR 164.512(i).

[6] *See* 45 CFR 160.103 (definition of "Protected health information").

[7] *See, e.g.*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites and https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2796236 .

[8] Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a).

[9] *See* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").

[10] 45 CFR part 160 and subparts A and E of part 164.

[11] This Bulletin uses the term "user-authenticated webpages" to refer to webpages that users can access only ***after*** they log in to the webpage, such as by entering a unique user ID and password or other credentials.

[12] This Bulletin uses the term “unauthenticated webpages” to refer to webpages that are publicly accessible without first requiring a user to log in to such webpage.

[13] A mobile app is a software program for mobile devices. This Bulletin uses the term “mobile apps” to refer to apps offered to individuals by regulated entities to allow the individuals to, for example, find providers, access or manage their health information or health care, or pay bills.

[14] *See* FTC Report on Cross-Device Tracking, https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017.

[15] Cookies are files placed on a user’s device to customize a user’s browsing experience but can also be used to track a user's activities. A web beacon or tracking pixel is a tiny graphic image (usually 1 pixel) placed on a webpage that allows the website owner or a third party to collect information regarding the use of the webpage that contains the web beacon. Session replay scripts record a user’s activities (*e.g.*, mouse movements, clicks, and typing) when using a webpage or app. Fingerprinting uses a browser’s and/or device’s unique configurations and settings to track user activity.

[16] A device ID is a unique string of numbers and letters associated with a smartphone or similar mobile device.

[17] An advertising ID is a unique string of numbers and letters assigned to smartphones or similar mobile devices that allows advertisers to track user activity.

[18] For additional information on the collection of sensitive information obtained from tracking technologies, *see* https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[19] Generally, individually identifiable health information is a subset of health information, including demographic information collected from an individual, that is received by a covered entity (or its business associate) or employer; relates to the past, present, or future health, health care, or payment for health care to an individual; and identifies the individual or can be used to identify the individual. *See* 45 CFR 160.103 (definition of “Individually identifiable health information”).

[20] For more information on identifiers under the Privacy Rule, *see* 45 CFR 164.514(b).

[21] There are limited situations in which an IP address or geographic location by itself may not be PHI, such as where the individual uses a computer at a public library instead of using their personal electronic device. This is because the IP address or geographic location will not be related to the individual when using a public device.

However, even in such cases, the IP address or geographic location from such devices, combined with any information provided by users through a webpage or mobile app, could be used to identify the individual and therefore may be PHI.

[22] *See* "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule", 78 FR 5566, 5598 (January 25, 2013).

[23] *See* 45 CFR 160.103 (definition of "Electronic protected health information").

[24] *See* 45 CFR part 164, subparts A and C.

[25] *See* 45 CFR 164.506; *see also* 45 CFR 164.501 (definition of "Health care operations").

[26] *See* 45 CFR 164.504(e) and 45 CFR 164.308(b).

[27] *See* OCR's Fact Sheet on Direct Liability of Business Associates, *supra* note 3.

[28] A health clinic is covered if it is a heath care provider that transmits any health information in electronic form in connection with a transaction covered by 45 CFR part 162.

[29] *See* 45 CFR 160.103 (definition of "Electronic media"); *see also* 45 CFR 160.103 (defining "Protected health information" as "individually identifiable health information . . . that is transmitted by electronic media; maintained by electronic media; or transmitted or maintained in any other form or medium").

[30] For additional resources for mobile health app developers, *see* https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html.

[31] A mobile device fingerprint typically includes information such as the device name, type, operating system version, and IP address.

[32] For more information on the privacy and security of personal consumer apps, *see* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

[33] *See* 45 CFR 164.502(a), 45 CFR 164.502(b), and 45 CFR 164.514(d).

[34] *See*, *e.g.*, https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf - PDF.

[35] *See* 45 CFR 164.502(a) and 164.502(e).

[36] *See, e.g.*, 45 CFR 164.308(b)(3) and 45 CFR 164.502(e)(2).

[37] *See, e.g.*, 45 CFR 164.504(e); and 45 CFR 164.314(a). *See also* OCR's Sample Business Associate Contract, https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[38] *See* 45 CFR 164.308.

[39] A regulated entity must implement encryption for ePHI in transit and at rest if it is a reasonable and appropriate safeguard. If it is not reasonable and appropriate, the regulated entity must document why not and implement an equivalent alternative measure if reasonable and appropriate. *See* 45 CFR 164.312(a)(2)(iv); 45 CFR 164.312(e)(2)(ii); and 45 CFR 164.306(d). *See also* OCR's HIPAA FAQ #2020, https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html.

[40] *See* 45 CFR 164.308(a)(4); 45 CFR 164.312(a); 45 CFR 164.312(b); and 45 CFR 164.312(d).

[41] *See* 45 CFR 164.402 (definition of "Breach").

[42] *See* 45 CFR 164.400 *et seq.* Impermissible disclosures of health information by non-HIPAA regulated entities may be subject to the FTC's Health Breach Notification Rule. *See* 16 CFR 318 *et seq.*

Content created by Office for Civil Rights (OCR)
December 1, 2022