

[HHS](#) [HIPAA Home](#) [For Professionals](#)

Navigate to:



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

*On June 20, 2024, the U.S. District Court for the Northern District of Texas issued an order declaring unlawful and vacating a portion of this guidance document. See *Am. Hosp. Ass’n v. Becerra*, — F. Supp. 3d —, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024). Specifically, the Court vacated the guidance to the extent it provides that HIPAA obligations are triggered in “circumstances where an online technology connects (1) an individual’s IP address with (2) a visit to a[n] [unauthenticated public webpage] addressing specific health conditions or healthcare providers.” *Id.* at \*2. HHS is evaluating its next steps in light of that order.*

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<sup>1</sup> and business associates<sup>2</sup> (“regulated entities”) under the HIPAA Privacy, Security, and Breach

Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”).<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> 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).<sup>6</sup> Some regulated entities may share sensitive information with tracking technology vendors and such sharing may involve unauthorized disclosures of PHI with such vendors.<sup>7</sup> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures<sup>8</sup> 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.<sup>9</sup>

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule<sup>10</sup> 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, OCR is providing this reminder that it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.

To this end, this Bulletin provides guidance for regulated entities to consider when contemplating the use of tracking technologies, including an 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<sup>11</sup>
  - Tracking on unauthenticated webpages<sup>12</sup>
  - Tracking within mobile apps<sup>13</sup>
  - 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 or their actions as they interact with a 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, improve the utility of webpages and apps, or allocate resources. For example, hospitals might use data analytics to determine how many IP addresses accessed webpages providing information about COVID-19 vaccines or treatment in a particular area, which in turn could help the hospitals make decisions about how to allocate their medical and other resources. 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,<sup>14</sup> 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<sup>15</sup> 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<sup>16</sup> or advertising ID.<sup>17</sup> 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.<sup>18</sup>

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?**

Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps. The information disclosed 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, device IDs, or any unique identifying code.<sup>19</sup> In some cases, the information disclosed may meet the definition of individually identifiable health information (IIHI),<sup>20</sup> which is a necessary pre-condition for information to meet the definition of PHI when it is transmitted or maintained by a regulated entity.

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 in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.<sup>21</sup> But 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 if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care.<sup>22</sup>

The information below highlights how the HIPAA Rules apply in the context of tracking on user-authenticated webpages and unauthenticated webpages, and within mobile apps.

### ***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)<sup>23</sup> collected through its website is protected and secured in accordance with the HIPAA Security Rule.<sup>24</sup>

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<sup>25</sup>) 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.<sup>26,27</sup> For example, if an individual makes an appointment through the website of a covered health clinic<sup>28</sup> 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, visiting hours, employment opportunities, or their policies and procedures. Tracking technologies on many unauthenticated webpages 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. Regulated entities are required to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits."<sup>29</sup> Thus, regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.

The examples below illustrate when certain visits to an unauthenticated webpage may or may not involve the disclosure of PHI.

Visits to unauthenticated webpages do not result in a disclosure of PHI to tracking technology vendor if the online tracking technologies on the webpages do not have access to information that relates to any individual's past, present, or future health, health care, or payment for health care.

- For example, where a user merely visits a hospital's webpage that provides information about the hospital's job postings or visiting hours, the collection and transmission of information showing such a visit to the webpage, along with the user's IP address, geographic location, or other identifying information showing their visit to that webpage, would not involve a disclosure of an individual's PHI to tracking technology vendor. This is true even if there is a reasonable basis to believe that the information can be used to identify the user who visited the webpage, because the online tracking technologies in this example did not have access to information about an individual's past, present, or future health, health care, or payment for health care.

Further, visits to unauthenticated webpages do not result in a disclosure of PHI to tracking technology vendor if the visit is not related to an individual's past, present, or future health, health care, or payment for health care.

- For example, if a student were writing a term paper on the changes in the availability of oncology services before and after the COVID-19 public health emergency, the collection and transmission of information showing that the student visited a hospital's webpage listing the oncology services provided by the hospital would not constitute a disclosure of PHI, even if the information could be used to identify the student.
- However, if an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care.

Tracking technologies on a regulated entity's unauthenticated webpage that permits individuals to schedule appointments or use a symptom-checker tool without entering credentials may have access to PHI in certain circumstances.

- For example, tracking technologies might collect an individual's email address, or reason for seeking health care typed or selected by an individual, when the individual visits a regulated entity's webpage and makes an appointment with a health care provider or enters symptoms in an online tool to obtain a health analysis. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply. This is because, unlike the general situation for many unauthenticated webpages, the information collected in this example meets the definition of IIHI.

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 meets the definition of IIHI.<sup>30</sup> 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 a disclosure of PHI and is subject to the HIPAA Rules.

### ***Tracking within mobile apps***

Mobile apps<sup>31</sup> 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,<sup>32</sup> network location, geolocation, device ID, or advertising ID. Such information collected by a regulated entity's mobile app generally is PHI and 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, a patient might use a health clinic's diabetes management mobile app to track health information such as glucose levels and insulin doses. In this example, the transmission of information to a tracking technology vendor as a result of using such app would be a disclosure of PHI



because the individual's use of the app is related to an individual's health condition (*i.e.*, diabetes) and that, together with any individually identifying information (*e.g.*, name, mobile number, IP address, device ID), meets the definition of IIHI.

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.<sup>33</sup>

### **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.<sup>34</sup>
- 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.<sup>35</sup> 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.<sup>36</sup>
- 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.<sup>37</sup> 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.<sup>38</sup>
  - If 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 regulated entity can choose to establish a BAA with another vendor, for example a Customer Data Platform<sup>39</sup> vendor, that will enter into a BAA with the regulated entity to de-identify online tracking information that includes PHI and then subsequently disclose only de-identified information to tracking technology vendors that are unwilling to enter into a BAA with a regulated entity.
  - If a regulated entity does not want to create a business associate relationship with a vendor that meets the definition of business associate, it cannot disclose PHI to such a vendor without individuals’ authorizations.

- Addressing the use of tracking technologies in the regulated entity's Risk Analysis and Risk Management processes,<sup>40</sup> 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;<sup>41</sup> enabling and using appropriate authentication, access, encryption, and audit controls when accessing ePHI maintained in the tracking technology vendor's infrastructure)<sup>42</sup> to protect the ePHI.
- Providing breach notification<sup>43</sup> 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.<sup>44</sup>

### **OCR's Enforcement Priorities**

Compliance with the Security Rule helps lower the risk of unauthorized access to ePHI collected through a regulated entity's website or mobile app that could lead to harm to individuals. Therefore, OCR is prioritizing compliance with the HIPAA Security Rule in investigations into the use of online tracking technologies. OCR's principal interest in this area is ensuring that regulated entities have identified, assessed, and mitigated the risks to ePHI when using online tracking technologies and have implemented the Security Rule requirements to ensure the confidentiality, integrity, and availability of ePHI. OCR investigations are fact-specific and may involve the review of technical information regarding a regulated entity's use of any tracking technologies. OCR considers all of the available evidence in determining compliance and remedies for potential noncompliance.

### **Filing a Privacy Complaint**

If you believe that your (or someone else's) health privacy rights have been violated, visit the OCR complaint portal at <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf> <<https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>> to file a complaint online.

DISCLAIMER: The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or the Departments' policies.

To obtain this information in an alternate format, contact the HHS Office for Civil Rights at (800) 368-1019, TDD toll-free: (800) 537-7697, or by emailing [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov). Language assistance services for OCR matters are available and provided free of charge.

## Resources

HIPAA Guidance:

- Health Apps: <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html> <<https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html>>
- Security Rule: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es>
- Cybersecurity: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>  
<<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>>
- Privacy Rule: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html> <<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html>>
- Business Associate Contracts: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html> <<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>>

For more information on health apps and online tracking, visit:

- FTC Guidance on online tracking: <https://consumer.ftc.gov/articles/how-protect-your-privacy-online> <<https://consumer.ftc.gov/articles/how-protect-your-privacy-online>>

- FTC Guidance for mobile health apps:
    - <https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool> <<https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool>>
    - <https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act> <<https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act>>
    - <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use> <<https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use>>
  - FTC Health Breach Notification Rule: <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule> <<https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>>
  - ONC’s Model Privacy Notice for technology developers: <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf> [PDF] <<https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>>
- 

## Endnotes:

<sup>1</sup> See 45 CFR 160.103 (definition of “Covered entity”).

<sup>2</sup> See 45 CFR 160.103 (definition of “Business associate”).

<sup>3</sup> 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> </hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>

<sup>4</sup> 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> </hipaa/for-professionals/breach-notification/index.html>.

<sup>5</sup> 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).

<sup>6</sup> See 45 CFR 160.103 (definition of “Protected health information”).

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

<sup>8</sup> 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).

<sup>9</sup> See 45 CFR 164.508(a)(3); *see also* 45 CFR 164.501 (definition of “Marketing”).

<sup>10</sup> 45 CFR part 160 and subparts A and E of part 164.

<sup>11</sup> 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.

<sup>12</sup> 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.

<sup>13</sup> 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.

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

<sup>15</sup> 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.

<sup>16</sup> A device ID is a unique string of numbers and letters associated with a smartphone or similar mobile device.

<sup>17</sup> 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.

<sup>18</sup> 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> <<https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>>.

<sup>19</sup> For more information on identifiers under the Privacy Rule, see 45 CFR 164.514(b).

<sup>20</sup> Generally, individually identifiable health information is a subset of health information, including demographic information collected from an individual, that is created or received by a covered entity (or its business associate) or employer; and relates to the past, present, or future health, health care, or payment for health care



of an individual; and identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. See 45 CFR 160.103 (definition of “Individually identifiable health information”).

<sup>21</sup> 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.

<sup>22</sup> 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).

<sup>23</sup> See 45 CFR 160.103 (definition of “Electronic protected health information”).

<sup>24</sup> See 45 CFR part 164, subparts A and C.

<sup>25</sup> See 45 CFR 164.506; see *also* 45 CFR 164.501 (definition of “Health care operations”).

<sup>26</sup> See 45 CFR 164.504(e) and 45 CFR 164.308(b).

<sup>27</sup> See OCR’s Fact Sheet on Direct Liability of Business Associates, *supra* note 3.

<sup>28</sup> A health clinic is covered if it is a health care provider that transmits any health information in electronic form in connection with a transaction covered by 45 CFR part 162.

<sup>29</sup> 45 CFR 164.306(a).

<sup>30</sup> 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”).

<sup>31</sup> For additional resources for mobile health app developers, see <https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html> </hipaa/for-professionals/special-topics/health-apps/index.html>.

<sup>32</sup> A mobile device fingerprint typically includes information such as the device name, type, operating system version, and IP address.

<sup>33</sup> 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> </hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html>.

<sup>34</sup> See 45 CFR 164.502(a), 45 CFR 164.502(b), and 45 CFR 164.514(d).

<sup>35</sup> See, e.g., <https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf> [PDF] <<https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf>>.

<sup>36</sup> See 45 CFR 164.502(a) and 164.502(e).

<sup>37</sup> See, e.g., 45 CFR 164.308(b)(3) and 45 CFR 164.502(e)(2).

<sup>38</sup> 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> </hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>.

<sup>39</sup> A Customer Data Platform (CDP) is software that can combine data from multiple sources regarding customer interactions with a company's online presence to support a company's analytic and customer experience analysis. Some CDP vendors may be willing to work with regulated entities as their business associates and enter into appropriate business associate agreements. Such CDP vendors may include services providing for de-identification of online tracking data that contains PHI.

<sup>40</sup> See 45 CFR 164.308.

<sup>41</sup> 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> </hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html>.

<sup>42</sup> See 45 CFR 164.308(a)(4); 45 CFR 164.312(a); 45 CFR 164.312(b); and 45 CFR 164.312(d).

<sup>43</sup> See 45 CFR 164.402 (definition of “Breach”).

<sup>44</sup> 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.*



UNITED STATES OF AMERICA  
Federal Trade Commission  
WASHINGTON, D.C. 20580

Office of the Chair

**STATEMENT OF THE COMMISSION**  
*On Breaches by Health Apps and Other Connected Devices*

**September 15, 2021**

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC’s Health Breach Notification Rule, 16 C.F.R. Part 318 (“the Rule”).<sup>1</sup>

The FTC’s Health Breach Notification Rule helps to ensure that entities who are not covered by the Health Insurance Portability and Accountability Act (“HIPAA”) nevertheless face accountability when consumers’ sensitive health information is compromised. Under the Rule’s requirements, vendors of personal health records (“PHR”) and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations. The Rule also covers service providers to these entities. In practical terms, this means that entities covered by the Rule who have experienced breaches cannot conceal this fact from those who have entrusted them with sensitive health information.

The Rule was issued more than a decade ago, but the explosion in health apps and connected devices makes its requirements with respect to them more important than ever. The FTC has advised mobile health apps to examine their obligations under the Rule,<sup>2</sup> including through the use of an interactive tool.<sup>3</sup> Yet the FTC has never enforced the Rule, and many appear to misunderstand its requirements. This Policy Statement serves to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches.

The Rule covers vendors of personal health records that contain individually identifiable health information created or received by health care providers. The Rule is triggered when such entities experience a “breach of security.”<sup>4</sup> Under the definitions cross-referenced by the Rule, the developer of a health app or connected device is a “health care provider” because it “furnish[es] health care services or supplies.”<sup>5</sup> When a health app, for example, discloses

---

<sup>1</sup> The Rule implements the requirements of the American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, codified at 42 U.S.C. § 17937.

<sup>2</sup> *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM’N, <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices> (last visited on Sept. 15, 2021).

<sup>3</sup> *Mobile Health Apps Interactive Tool*, FED. TRADE COMM’N, <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool> (last visited on Sept. 15, 2021).

<sup>4</sup> See 16 C.F.R. § 318.2(a).

<sup>5</sup> See *id.* § 318.2; 42 U.S.C. § 1320d(6), d(3).

sensitive health information without users' authorization, this is a "breach of security" under the Rule.<sup>6</sup>

The statute directing the FTC to promulgate the Rule requires that a "personal health record" be an electronic record that can be drawn from multiple sources. The Commission considers apps covered by the Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces ("APIs"). For example, an app is covered if it collects information directly from consumers and has the technical capacity to draw information through an API that enables syncing with a consumer's fitness tracker. Similarly, an app that draws information from multiple sources is covered, even if the health information comes from only one source. For example, if a blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar), it is covered under the Rule.

In addition, the Commission reminds entities offering services covered by the Rule that a "breach" is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule.

As many Americans turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas, this Rule is more important than ever. Firms offering these services should take appropriate care to secure and protect consumer data. The Commission intends to bring actions to enforce the Rule consistent with this Policy Statement. Violations of the Rule face civil penalties of \$43,792 per violation per day.

---

<sup>6</sup> *Id.* § 318.2(a) (defining "breach of security" as "acquisition of [PHR identifiable health information] without the authorization of the individual.").



# Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule

**Tags:** [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#) | [Health Privacy](#)

Does your business collect, use, or share consumer health information? When it comes to privacy and security, you've probably thought about the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules). But did you know you also may need to comply with the Federal Trade Commission Act and the FTC's Health Breach Notification Rule? Learn more about your obligations under these laws to maintain the privacy and security of consumers' health information and provide notification if you experience a breach.

## HIPAA

Let's start with HIPAA. The HIPAA Rules apply to you if you are a HIPAA [covered entity](#) – a health plan, a health care provider that conducts standard health care transactions electronically, or a health care clearinghouse. Parts of the HIPAA Rules also apply if you are a [business associate](#) – a company or other entity that helps a covered entity carry out its health care activities and functions or provides certain services to a covered entity or another business associate involving access to individuals' "protected health information" (PHI). PHI is most "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, paper, or oral.

The [HIPAA Privacy Rule](#) sets limits and conditions on the uses and disclosures of PHI that covered entities and business associates may make without an individual's authorization and provides individuals with rights with respect to their health information. Under the Privacy Rule, a cover



entity or business associate must obtain an individual's valid HIPAA authorization to use or disclose the individual's PHI for marketing purposes. Here are some highlights of the Privacy Rule's requirements for an authorization when one is required:

- **Get the individual's signed authorization before making the use or disclosure.** You can obtain an individual's authorization electronically or in non-electronic form. With limited exceptions, you cannot condition your provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the individual providing an authorization for the use or disclosure of their PHI.
- **Put it in plain language.** HIPAA authorizations provide individuals a way to understand and control uses and disclosures of their health information. The authorization must be in **plain language**. If people can't understand it, it is not effective. Explain who is being authorized to make the use or disclosure, what information will be used or disclosed, who will receive the information, when the permission expires, and the purpose for which the information will be used and disclosed.
- **Be specific in your description of how you want to use or disclose health information.** The authorization must describe the specific purpose for a requested use or disclosure. For example, if you want an individual to authorize you to share their health information, you need to tell them specifically how it will be used and disclosed – for example, by a pharmaceutical company for marketing purposes, a life insurer for coverage purposes, or an employer for screening purposes.
- **If you will benefit financially from a disclosure, clearly say so in the authorization.** The Privacy Rule prohibits you from selling PHI unless you obtain an authorization stating that you will receive remuneration from making the disclosure.

If you are a business associate, there's a crucial first step. **The covered entity must give you permission through a [HIPAA business associate agreement](#) for any** use or disclosure of PHI. This means you cannot ask an individual to sign a HIPAA authorization unless your business associate agreement permits you to do so.

The [HIPAA Security Rule](#) requires HIPAA covered entities and their business associates to implement safeguards to protect the confidentiality, integrity, and availability of all electronic PHI (ePHI) the covered entity or business associate creates, receives, maintains, or transmits. Examples of safeguards established by the Security Rule include:



- Identifying potential risks and vulnerabilities to ePHI and implementing security measures to reduce those risks and vulnerabilities.
- Providing security awareness and training to all workforce members.
- Establishing contingency plans that include backing up ePHI data and disaster recovery.
- Identifying and responding to suspected or known security incidents.
- Using access controls to limit access to ePHI to only authorized workforce members.
- Implementing encryption to protect ePHI where reasonable and appropriate.
- Maintaining audit controls and reviewing information system activity.

The [HIPAA Breach Notification Rule](#) requires HIPAA covered entities to [provide notification](#) to affected individuals, [the Secretary of HHS](#), and, in some cases, the media, following a breach of unsecured PHI. The Breach Notification Rule also requires business associates to notify the covered entity if the business associate experiences such a breach. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in [guidance](#).

Breach reports to the Secretary of HHS must be submitted through [OCR's breach portal](#). The breach portal also includes a [list of breaches affecting 500 or more individuals](#).

## FTC Act

The FTC Act prohibits companies and individuals from engaging in unfair or deceptive acts or practices in or affecting commerce. This means you must ensure your health data practices aren't substantially injuring consumers, including by invading their privacy. It also means that you must not mislead consumers about – among other things – what's happening with their health information. The FTC Act's obligations apply to HIPAA-covered entities and business associates, as well as to companies that collect, use, or share health information that aren't required to comply with HIPAA.

Practically speaking, what does that mean? As an initial matter, consider whether your practices cause harm to consumers or are likely to harm them. Where consumers can't reasonably avoid [↑](#) likelihood of substantial injury and the benefits to consumers or competition don't outweigh it, the



FTC can challenge the practice as unfair. For instance, [BetterHelp](#), [GoodRx](#), and [Premom](#) make clear that disclosing consumers' health information for advertising without their affirmative express consent may be an unfair practice.

Consider everything your business says or implies to consumers about the use, collection, retention, or sharing of their health data – and anything material you *fail* to say – to make sure you don't create a deceptive or misleading impression. For example, if you're covered by HIPAA and the information surrounding your HIPAA authorization is deceptive or misleading (such as by implying that to receive treatment, the consumer must agree to have their data used for advertising purposes), that's a violation of the FTC Act. Or if you use behind-the-scenes tracking technologies that share consumers' sensitive health data in contradiction of your privacy promises, that's a violation of the FTC Act.

### Other Key Points about How the FTC Act Applies to Health Information

- **"Health information" includes more than treatments and diagnoses.** Rather, it's anything that conveys information or enables an inference about a consumer's health. For example, browsing information, location information (e.g., data showing a consumer visited a cancer center) or purchase information (e.g., data showing a consumer purchased a home pregnancy test) can convey health information. To avoid violating the FTC Act, take a broad view of what constitutes health data and handle it accordingly.
- **The privacy of health information is a priority for consumers – and the FTC.** The FTC Act requires you to take privacy and security into account while collecting, using, retaining, and disclosing consumers' health information. It is critical that you understand your data flows. What health information are you collecting? From what sources? How are you using it? To whom are you disclosing it? For what purposes? How long are you retaining it and why? You must also establish strong privacy practices and implement robust safeguards to protect the privacy and security of the health information. This should include maintaining a written program to protect health information, conducting appropriate training and supervision, and implementing policies that address data retention, purpose, and use limitations; and (where appropriate) ensuring that any consent consumers provide is meaningful, informed, and not the product of deceit or coercion. You should also periodically review your practices and safeguards to make sure they are working effectively, not causing harm to consumers, and still line up with the privacy claims you've made.
- **Representations to consumers must be consistent with your practices and clear and conspicuous.** Review your entire user interface from the consumer's point of



view, including any claims made about health information. For example, as noted in [other FTC business guidance](#), don't make false or misleading claims that you are "HIPAA Compliant," "HIPAA Secure," "HIPAA Certified" or the like. Also, be upfront about your practices, tell consumers the whole truth, and don't bury key facts in a privacy policy, a Terms of Use section, or other places where consumers aren't likely to read and understand them. Evaluate the size, color, and graphics of all your statements to consumers to ensure they are clear and conspicuous.

## FTC's Health Breach Notification Rule

The [Health Breach Notification Rule](#) applies to certain businesses or organizations that aren't covered by HIPAA – specifically, vendors of personal health records (PHR), PHR related entities, and third party service providers. Do you have a mobile app, website, Internet-connected device, or similar technology that holds consumers' electronic health information in a personal health record? Do you provide products or services or send or receive data to or from that kind of product? Do you deal with health information while providing services to companies that offer those products? If so, you may be required to comply with this Rule.

If you experience a breach of security of consumers' identifying health information the Health Breach Notification Rule requires you to notify affected consumers, the FTC, and, in some cases, the media. A "breach of security" under the Rule includes an unauthorized acquisition of identifiable health information that occurs as a result of a data security breach *or* an unauthorized disclosure by the company itself.

The FTC's Health Breach Notification Rule applies only to identifying health information that is not secured through technologies specified by the Department of Health and Human Services.

### WHAT CAN YOU DO TO COMPLY WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE?

- **Understand your obligations under the Health Breach Notification Rule.** Review [Complying with the FTC's Health Breach Notification Rule](#), which explains who's covered by the Rule and offers guidance on what to do in case of a breach.
- **Report breaches in a timely fashion.** You must timely report breaches to the FTC using the online [Notice of Breach of Health Information](#). The FTC periodically posts a [list of breaches](#) involving the information of 500 or more individuals. Failing to make the necessary notifications or failing to make timely notifications as required by the Rule could result in an enforcement action and significant civil penalties.



If you have a health app, consult the [mobile health app interactive tool](#), the [FTC's best practices guidance for mobile health app developers](#), and the [HHS Office for Civil Rights' resources for mobile health apps developers](#). And when you're telling consumers about how you share consumer health information, keep the FTC Act, the FTC's Health Breach Notification Rule, and the HIPAA Rules in mind.

## About the FTC

The FTC works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers. Report scams and bad business practices at [ReportFraud.ftc.gov](#). We also provide guidance at [business.ftc.gov](#) to help companies comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Looking for a quick take on recent cases and other initiatives? Subscribe to the FTC's Business Blog at [ftc.gov/businessalerts](#).

## Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to [www.sba.gov/ombudsman](#).

**August 2024**

