

Managing Risk with Online Tracking Technology on Healthcare Websites

prepared for

New Jersey Hospital Association

July 19, 2023



Attorneys at
Oscislowski LLC

What Are We Going to Cover?

- **How it Started**

- Online Tracking Tools
- Mass General Settlement
- Markup Expose'

- **How it's Going**

- Breach Notifications re: Online Tracking
- Class Actions
- OCR Guidance
- Definitions: "PHI" and "IIHI"
- Deidentification
- OCR HIPAA Investigations

- **Moving Forward**

- AHA Pushes Back
- FTC Enforcement
- Compliance Approach



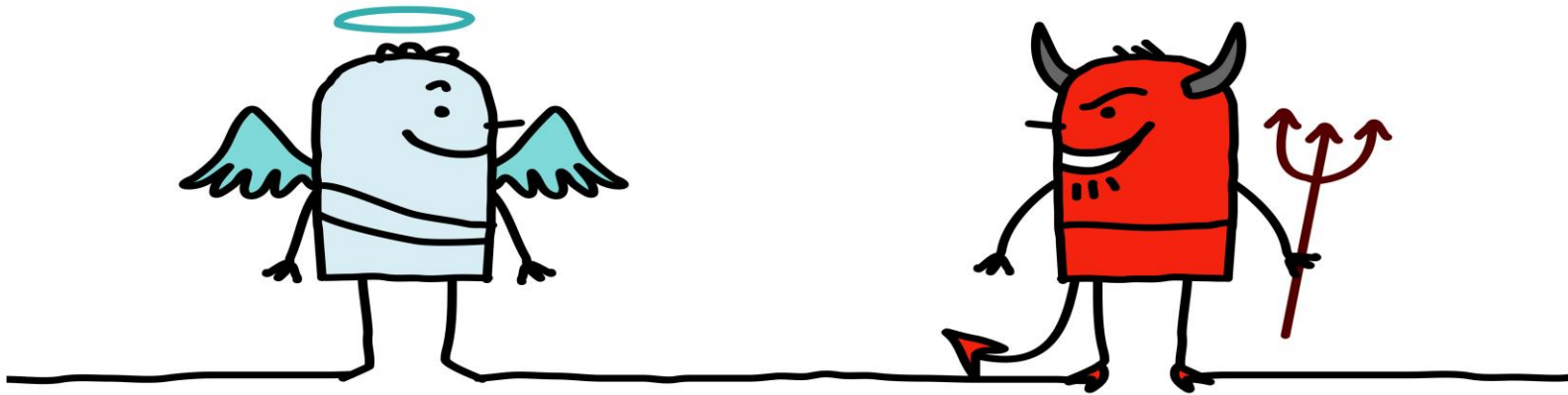
How it Started

Online Tracking Technologies

Online tracking technologies ***enabled*** by hospitals, health care providers etc. to collect and analyze information about user behavior and improve website functionality.

Google -- ***Google Analytics***

FaceBook/Meta -- ***Meta Pixel***



Mass General Brigham & Dana-Farber Cancer Institute 18.4 Million Settlement

**BOSTON
BUSINESS JOURNAL**

INSIDER VIEW
Candid Conversations with Forward Thinking Leaders >

Banking Technology Health Care Residential Real Estate BostInno | Events Nominations



The Dana-Farber Cancer Institute at 450 Brookline Avenue.
BOSTON BUSINESS JOURNAL

By **Jessica Bennett** – Reporter, Boston Business Journal
Jan 6, 2022

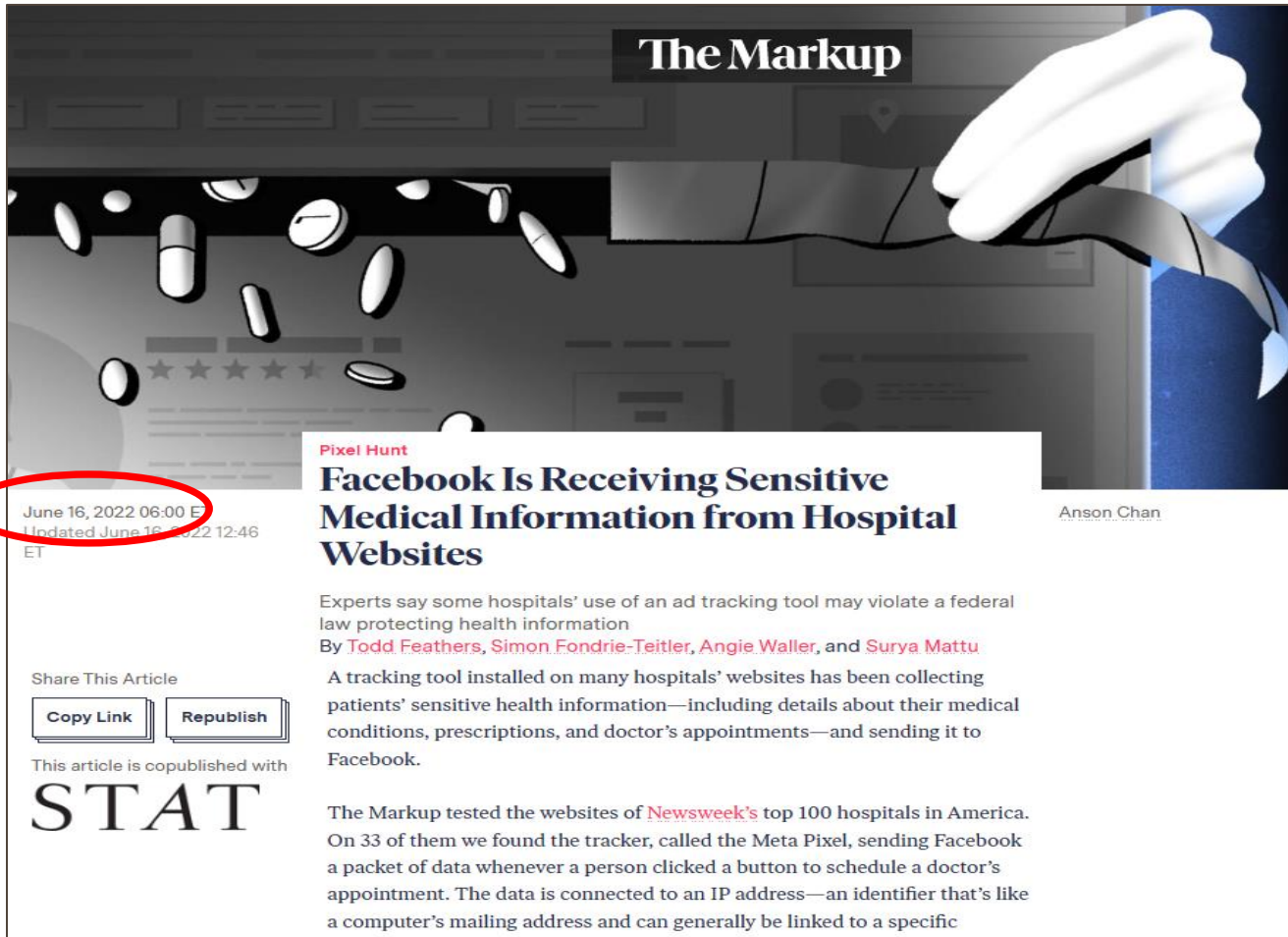
IN THIS ARTICLE

Hospitals
Topic

Mass General Brigham and Dana-Farber Cancer Institute have agreed to pay a combined \$18.4 million settlement over allegations that the institutions fed personally identifiable information about patients to Facebook, Google and other companies.



The “Markup” Exposé’



The Markup

June 16, 2022 06:00 ET
Updated June 16, 2022 12:46 ET

Pixel Hunt
Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Anson Chan

Experts say some hospitals’ use of an ad tracking tool may violate a federal law protecting health information
By [Todd Feathers](#), [Simon Fondrie-Teitler](#), [Angie Waller](#), and [Surya Mattu](#)

A tracking tool installed on many hospitals’ websites has been collecting patients’ sensitive health information—including details about their medical conditions, prescriptions, and doctor’s appointments—and sending it to Facebook.

The Markup tested the websites of [Newsweek’s](#) top 100 hospitals in America. On 33 of them we found the tracker, called the Meta Pixel, sending Facebook a packet of data whenever a person clicked a button to schedule a doctor’s appointment. The data is connected to an IP address—an identifier that’s like a computer’s mailing address and can generally be linked to a specific

Share This Article
[Copy Link](#) [Republish](#)

This article is copublished with
STAT

Credit: T. Feathers et al., “Facebook Is Receiving Sensitive Medical Information from Hospital Websites,” The Markup (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-website>



MetaPixel found on 33 of Newsweek Top 100 Hospitals

Atrium Health Carolinas Medical Center	Johns Hopkins Bayview Medical Center	Memorial Care Long Beach Medical Center	Scripps Memorial Hospital La Jolla	University Hospitals Cleveland Medical Center
Auroral St. Luke's Medical Center	Inova Fairfax Hospital	Loyola University Medical Center	Sharp Memorial Hospital	Unity Point Health – Meriter
Barnes-Jewish Hospital	Houston Methodist Hospital	New York Presbyterian Hospital	St. Joseph Mercy Chelsea	University of Chicago Medical Center
Brigham and Women's Faulkner Hospital	Hospital of the University of Pennsylvania	Northwestern Medicine Central DuPage Hospital	Tampa General Hospital	University of Iowa Hospitals and Clinics
Duke University Hospital	Johns Hopkins Hospital	Northwestern Memorial Hospital	Tufts Medical Center	UPMC Presbyterian & Shadyside
El Camino Hospital	Henry Ford Hospital	Sanford USD Medical Center	UCLA Reagan Medical Center	UT Southwestern Medical Center
Froedtert Hospital & the Medical College of Wisconsin	Jefferson Health – Thomas Jefferson University Hospitals	Penn Medicine Chester County Hospital	Source: Newsweek, The Markup	



“Meta Pixel collects Sensitive PHI”

The Meta Pixel collects sensitive health information and shares it with Facebook



The Meta Pixel installed on Piedmont Healthcare’s MyChart portal sent Facebook details about a real patient’s upcoming doctor’s appointment, including date, time, the patient’s name, and the name of their doctor

- 1 Patient name
- 2 Date and time of appointment
- 3 Name of provider

```
{“classList” : “_Link+_actionable+_link+_readOnlyText+_InternalLink+main”, “destination” : “https://mychart.piedmont.org/PRD/app/communication-center/conversation?id=ID REDACTED BY THE MARKUP”, “id” : “”, “imageUrl” : “/PRD/en-US/images/ProviderSilhouette.png”, “innerText” : “MyChart+Messaging+User\nREDACTED BY THE MARKUP\nAppointment+scheduled+from+MyChart\nThere+is+a+message+in+this+conversation+that+has+not+yet+been+viewed.\n 1 Appointment+For:+NAME REDACTED BY THE MARKUP+(ID REDACTED BY THE MARKUP)+Visit+Type:+NEW+PATIENT+(ID REDACTED BY THE MARKUP)+ 2 MM/DD/YYYY+0:00+XX+00+mins.+ 3 NAME REDACTED BY THE MARKUP,+MD”, “numChildButtons” : 0, “tag” : “a”, “name” : “”}
```

Source: mychart.piedmont.org, Mozilla Rally

Credit: T. Feathers et al., “Facebook Is Receiving Sensitive Medical Information from Hospital Websites,” The Markup (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>



Meta Pixel on Scheduling Pages

Pixel tracking found on appointment

Pixel tracking removed from appointment scheduling page after

On the website of University Hospitals Cleveland Medical Center, for example, clicking the “Schedule Online” button on a doctor’s page prompted the Meta Pixel to send Facebook the text of the button, the doctor’s name, and the search term we used to find her: “pregnancy termination.”

Duke University Hospital

Yes

No

Link

Did not respond

Source: Newsweek, The Markup - [Get the data](#)



Meta Pixel on Patient Portals

Health Systems with Meta Pixels on Their Patient Portals

The Markup identified seven health systems that had installed pixels inside their password-protected patient portals. Data accurate as of as of June 15, 2022.

Hospital	Pixel removed after being contacted by The Markup	Hospital comment
Community Health Network	Yes	Link
Edward-Elmhurst Health	Yes	Did not respond
FastMed	No	Did not respond
Novant Health	Yes	Link
Piedmont	Yes	Did not respond
Renown Health	Unknown	Did not respond
WakeMed	Yes	Did not respond

Source: Mozilla Rally, The Markup - [Get the data](#)



How it's Going

The Fallout . . .

- Breach Notices
- Class Action Lawsuits
- OCR Guidance
- OCR Investigations



The Fallout: Breach Notices

Healthcare Providers begin notifying patients regarding use of tracking technologies:

WakeMed

Home › About Us › News & Media

WakeMed News

Current Releases

10/14/2022

RALEIGH, N.C. (October 14, 2022) - Protecting patient information is a top priority. In support of WakeMed's core values, we are taking steps to ensure that some patients of the potential that select error.

WakeMed, like most companies, uses technology to enhance the patient experience. Anonymous user information is through a user visits a website, which allows certain


In March 2018, WakeMed placed pixel, provided by Meta, Google, and other tech companies have been facing backlash over the use of tracking pixels on healthcare websites.

Unfortunately, the pixel's software code may have resulted in the exposure of patient information. We are currently reviewing the scheduling page back to Facebook.

<https://wakemed.org/about-us/patients-of-potential-data-privacy>

Tracking Pixel Use Results in Data Breach at NY Hospital, 54K Impacted

The use of tracking and analytics tools on NewYork-Presbyterian Hospital's public-facing website may have resulted in the exposure of patient information.



Source: Getty Images

By Jill McKeon

April 04, 2023 - NewYork-Presbyterian Hospital (NYP) is the latest healthcare organization to report a **data breach** stemming from its use of tracking and analytics tools. As previously reported, Meta, Google, and other tech companies have been facing backlash over the use of tracking pixels on healthcare websites.

In October 2022, Advocate Aurora Health **notified 3 million individuals** of a breach stemming from the use of tracking pixels, and Novant Health **notified 1.3 million individuals** of potential unauthorized data disclosures resulting from its use of pixels.

In the case of NewYork-Presbyterian Hospital, more than 54,000 individuals were recently notified that the use of third-party tracking and analytics tools on its public-facing website may have resulted in the exposure of patient information.

BY Health Science Oddities Lifestyle

The data tracker

Illinois

g

te

type

ents



The Fallout: Class Action Lawsuits

www.beckershospitalreview.com/healthcare-information-technology/9-hospitals-health-systems-facing-lawsuits-for-healthcare-data-sharing.html

The screenshot shows a news article on the Becker's Hospital Review website. At the top, there is a navigation bar with 'HEALTH IT' and 'HOSPITAL REVIEW' logos. A blue banner below the navigation bar reads 'Engage, Network & Learn with thousands of your executive peers: Apply to be a live conference reviewer' with an 'APPLY NOW' button. Below the banner is a menu with categories: E-Newsletters, Conferences, Virtual Conferences, Webinars, Whitepapers, Podcasts, and Print Issues. A secondary navigation bar lists topics: Cybersecurity, EHRs, Telehealth, Innovation, Digital Health, Disruptors, and Marketing. The main headline is '18 hospitals, health systems facing lawsuits for healthcare data-sharing' in bold black text. Below the headline is the author 'Naomi Diaz' and the date 'Updated Wednesday, April 26th, 2023'. A row of social media icons (heart, Facebook, Twitter, LinkedIn, YouTube, RSS, Print, Email) is displayed. The article text begins with 'Hospitals and health systems around the country have been accused of sharing confidential patient information with social media giants such as Meta, Facebook and Google. Here are the 18 hospitals and health systems facing lawsuits for alleging sharing healthcare data for marketing purposes:'. An 'Editor's note' states: 'This article was updated on April 26 and will be continuously updated.' A yellow highlighted section titled 'April 26:' contains a bulleted list of four lawsuits: 1. A lawsuit filed against University of Iowa Hospitals & Clinics alleges that the health system installed pixel tracking technology on its websites that shared patient data with Facebook. 2. A lawsuit claims that Greensburg, Pa.-based Excelsior Health improperly disclosed patients' protected health information to Facebook and Google after it allegedly used tracking technology on its web portal. 3. A lawsuit alleges that State College, Pa.-based Mount Nittany Health used pixels on its website that sent some patients' protected health information to Facebook and Google. 4. A lawsuit filed April 3 alleges that Dallas-based Steward Health Care System's website used a Meta pixel tracking tool that sent some patient information to Meta and Google.

December 2022 OCR Guidance


www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for...  [A-Z Index](#)

[HIPAA for Individuals](#) [Filing a Complaint](#) [HIPAA for Professionals](#) [Newsroom](#)

[HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates](#)

Text Resize  Print  Share 

HIPAA for Professionals

Regulatory Initiatives

Privacy

- Summary of the Privacy Rule
- Guidance
- Combined Text of All Rules
- HIPAA Related Links

Security

Breach Notification

Compliance & Enforcement

Special Topics

Patient Safety

Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules

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 entities¹ and business associates² ("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 disclosures⁸ 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 Rule¹⁰ 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?

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 webpages¹¹
 - Tracking on unauthenticated webpages¹²
 - Tracking within mobile apps¹³
 - 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 scripts¹⁵ 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 ID¹⁶ 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

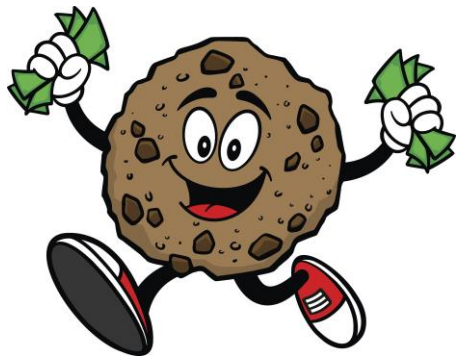
Website or mobile app owners may use tracking technologies developed internally or those developed by third parties. Generally, tracking technologies developed by third parties (e.g., tracking technology vendors) send information directly to the third parties who developed such technologies and may continue 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 Technology”

OCR generally describes online tracking technology as “a **script** or **a code** on a website or a mobile app used to **gather information about users** as they interact with the website or mobile app.”



- Cookies
- Tracking Pixels
- Web beacons
- Session replay scripts
- Fingerprinting scripts
- **Mobile Apps** include/embed tracking code within the App to enable the app to collect information directly provided by the user e.g., **device ID** or **advertising ID**

Google Analytics and Meta Pixel (for Facebook) are two examples of widely-used tracking technologies.



Three Buckets

1. User-authenticated webpages
2. Unauthenticated webpages
3. Mobile Apps

User-authenticated webpages

- Require a user to **log in** *before* they are even able to access the webpage
- *Examples:* Patient portals and telehealth platforms
- If enabled, **likely** to have access to specific PHI



Unauthenticated webpages

- Do **not require** users to log in to access the webpage
- Webpages with *general* information (i.e., services)
- Although these webpages typically do *not* include access to individuals' PHI, OCR also highlights **exceptions**:
 - ***Permits a user to enter information***, such as demographic info, scheduling info, registration info etc.;
 - Addresses ***specific symptoms or health conditions***, such as pregnancy or miscarriage;
 - Permits individuals to ***search for doctors or schedule appointments*** without entering log-in credentials.



Mobile Applications

Mobile apps that are not “*offered by or on behalf of*” a regulated entity (i.e., ones that individuals use to request and download their own information from a regulated entity) would not be subject to HIPAA.



OCR's Interpretation of "PHI"

“Individually identifiable health information (IIHI) that the individual provides when they **use regulated entities' websites or mobile apps** . . . 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.

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.”*



Wait ... What??!!



“Protected Health Information”

- **Individually identifiable health information** that is transmitted by or maintained in **electronic media**, or transmitted or maintained in any other form or medium.
- Excludes
 - FERPA
 - Records in 20 USC 1232g(a)(4)(B)(iv)
 - Employment records held by a covered entity in its role as employer
 - PHI about a person who has been deceased for more than 50 years



“Electronic Media”

- Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;
- **Transmission media** used to exchange information already in electronic storage media. Transmission media include, for example, **the Internet**, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.
 - CONDUIT EXCEPTION: Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via *electronic media* if the information being exchanged did not exist in electronic form immediately before the transmission.

“Individually Identifiable Health Information”

A subset of *health information*, including demographic information, **collected from** an individual, **and**

- Is created or **received by** a health care provider, health plan, employer, or health care clearinghouse; **and**
- **Relates to** the *past, present, or future physical or mental health or condition of an individual* **OR** the provision of health care to an individual **OR** the past, present, or future payment for the provision of health care to an individual; **and**
 - That ***identifies*** the individual; or
 - With respect to which there is a ***reasonable basis*** to believe the information can be used to ***identify*** the individual.

“Health Information”

Means any information, including genetic information, whether oral or recorded in any form or medium, that:

- (1) Is created or **received by** a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (2) **Relates to** the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.



Incidental Disclosures

Covered Entity is **permitted** to use or **disclose PHI** as follows:

- To the Individual;
- TPO (in accordance with 164.506)
- **Incident to** a use or disclosure otherwise permitted or required by the Privacy Rule, provided that the CE has complied with the applicable requirements of ***Minimum Necessary*** and has in place “appropriate administrative, technical and physical ***Safeguards*** to **protect the privacy of PHI** with respect to such otherwise permitted or required use or disclosure; [...]”



Deidentification “Safe Harbor”

45 CFR 164.514(b)(2): the following identifiers of the *individual* & individual’s *relatives*, employers or *household members*, must be removed:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from Census: (i) geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; & (ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- **Web Universal Resource Locators (URLs);**
- **Internet Protocol (IP) address numbers;**
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- **Any other unique identifying number, characteristic, or code (except as permitted by paragraph (c))**



Expert Method

45 CFR 164.514(b)(1)

Analysis and **certification by an expert** as follows:

- Must be performed by a person (the Expert) with appropriate knowledge of & experience with generally accepted statistical and scientific principles & methods for rendering information not individually identifiable;
- The Expert must apply such principles & methods and **determines that the risk is very small** that the info could be used, alone or in combination with other reasonably available info, by an anticipated recipient to **identify an individual** who is a subject of the information; and
- The Expert documents the methods and results of the analysis that justifies such determination.



HHS Interpretation = a Slippery Slope



NJ071923EDU

OCR Investigations are Underway



OCR Information Request

INITIAL DATA REQUEST

In connection with OCR's investigation, we request that [ENTITY] provide the following information to OCR within thirty (30) calendar days from receipt of this letter. If you believe that [ENTITY] is not a HIPAA covered entity or business associate, please complete and return only Part I of the Data Request. Otherwise, please complete Parts I and II of the attached Data Request.

Please answer each question fully and in detail. Please number responses and attachments to correspond with the enumerated requests. Please submit each response (with attachments) to each enumerated question as a separate Word or PDF document and label each document accordingly (e.g., "Part I, Q1" or "Part I, Q2," etc.).

PART ONE:

The HIPAA Privacy Rule applies to "covered entities" as defined by 45 C.F.R. § 160.103: Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by the standards found in 45 C.F.R. Parts 160 and 162.

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- (1) Health care claims or equivalent encounter information.
- (2) Health care payment and remittance advice.
- (3) Coordination of benefits.
- (4) Health care claim status.
- (5) Enrollment and disenrollment in a health plan.
- (6) Eligibility for a health plan.
- (7) Health plan premium payments.
- (8) Referral certification and authorization.
- (9) First report of injury.
- (10) Health claims attachments.
- (11) Health care electronic funds transfers (EFT) and remittance advice.
- (12) Other transactions that the Secretary may prescribe by regulation.

For more information on "covered entities," visit:
<https://www.hhs.gov/hipaa/forprofessionals/covered-entities/index.html>

OCR also has jurisdiction over "business associates" as defined by 45 C.F.R. 160.103. A "business associate" is a person or entity that creates, receives, maintains, or transmits protected health information for a covered function or provides certain services to or for such covered entity or associate includes the disclosure of protected health information.

For more information on "business associates," visit:
<https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/business-associates/index.html>

Please respond to the following:

1. Does [ENTITY] transmit any of the following standard (HIPAA) transactions, or contract with a billing service or clearinghouse to do so on its behalf?

	YES	NO
A. Claims or Equivalent Encounter Information (ASC form 837) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B. Payment and Remittance Advices (ASC form 835) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
C. Claim Status Inquiry and Responses (ASC form 276/277) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D. Eligibility Inquiry and Responses (ASC form 270/271) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E. Referral Certification and Authorization Inquiry and Response (ASC form 278) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F. Health Plan Premium Payments (ASC form 820) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G. Coordination of Benefits (ASC form 837) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Which of the following methods does [ENTITY], or any billing service or clearinghouse it contracts with, use to transmit each of the above type of transactions?

A. Electronic Data Interchange (EDI) Technology <input type="checkbox"/>	<input type="checkbox"/>
B. Internet and Web-based Applications <input type="checkbox"/>	<input type="checkbox"/>
C. Direct Data Entry (DDE) Modem <input type="checkbox"/>	<input type="checkbox"/>
D. Sending a Diskette/Tape <input type="checkbox"/>	<input type="checkbox"/>
E. Using a Credit Card Swipe Machine (Point of Service or POS) <input type="checkbox"/>	<input type="checkbox"/>
F. Using "Faxback" Telephone Voice Response <input type="checkbox"/>	<input type="checkbox"/>
G. Paper Forms <input type="checkbox"/>	<input type="checkbox"/>
H. Dedicated Line Fax Machine <input type="checkbox"/>	<input type="checkbox"/>
I. Telephone <input type="checkbox"/>	<input type="checkbox"/>

3. Has [ENTITY] been issued a National Provider Identifier (NPI) by the Centers for Medicaid and Medicare Services ("CMS")? If yes, what is [ENTITY]'s NPI?



Moving Forward

AHA Pushes Back

www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance



Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4856
(202) 638-1100

May 22, 2023

Melanie Fontes Rainer
Director, Office for Civil Rights
Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W., Room 515F
Washington, DC 20201

Re: HIPAA Privacy Rule to Support Reproductive Health Care Privacy; 88 Fed. Reg. 23506 (RIN 0945-AA20) (April 17, 2023)

Dear Director Fontes Rainer:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinical partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) strongly supports the Office of Civil Rights' (OCR) proposed rule. The AHA agrees with OCR that a "positive, trusting relationship between individuals and their health care providers is essential to an individual's health and well-being."¹ **The proposed rule will enhance provider-patient relationships by providing heightened privacy protections for information about care that is lawful under the circumstances in which it is provided, but may nonetheless get swept up in criminal, civil or administrative investigations.**

At the same time, the AHA has serious concerns about a recent, related OCR policy: the December 2022 guidance on the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" (hereinafter "Online Tracking Guidance"). This guidance — ostensibly issued with the same worthy goal in mind as the proposed rule — is too broad and will result in significant adverse consequences for hospitals, patients and the public at large. **In particular, by treating a mere IP address as protected health information under HIPAA, the Online Tracking Guidance will reduce public access to credible health information.**

¹ 88 C.F.R. 23506, 23508.



Director Fontes Rainer
May 22, 2023
Page 4 of 8

In December 2022, OCR issued guidance regarding the use of online tracking technologies, *i.e.*, technologies that are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications. The AHA understands that this guidance may have been motivated — at least in part — by the same concerns as the proposed rule.⁴ **Regrettably, the Online Tracking Guidance errs by defining PHI too broadly — specifically, to include all IP addresses.⁵ As a result, the guidance will inadvertently impair access to credible health information. It should be suspended or amended immediately.**

Americans are increasingly reliant on digital platforms for health information. According to a March 2023 report by the National Quality Forum, "[a]pproximately 74 percent of surveyed Americans use search engines to start their patient journey."⁶ But online health information "can be disconcerting, confusing, and even misleading, leaving the onus on the consumer to decipher the information."⁷ And as Surgeon General Vivek H. Murthy recently explained, "Health misinformation is a serious threat to public health. It can cause confusion, sow mistrust, harm people's health, and undermine public health efforts. Limiting the spread of health misinformation is a moral and civic imperative that will require a whole-of-society effort."⁸

It is therefore critical that consumers who use the internet to obtain health information visit trustworthy, helpful and accurate sources. Hospitals and health systems play an important role in this regard. Our members' digital platforms are typically the best sources of health information. For this reason, Surgeon General Murthy specifically recommended that medical professionals, like our hospital and health system members, use "technology and media platforms to share accurate health information with the

⁴ See, e.g., United States Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (Dec. 1, 2022), at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#fnref22> ("Examples of unauthenticated webpages where the HIPAA Rules apply include ... [t]racking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage."); *id.* ("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).");

⁵ As you know, an IP address is simply a long string of numbers assigned to every device connected to a network that uses the Internet. Critically, the IP address identifies the computer, smart phone, tablet or other device, whether it is in someone's home, office, a public library, apartment building or somewhere else. As such, that device could be associated with a particular person or it could be shared by many different people.

⁶ National Quality Forum, *Issue Brief: Improving the Accessibility of High Quality Online Health Information 1* (Mar. 14, 2023), https://www.einnews.com/pr_news/622101919/high-quality-health-info-online-must-be-accessible-says-issue-brief-from-nqf-with-support-from-youtube-health (hereinafter National Quality Forum Study).

⁷ *Id.*

⁸ Vivek H. Murthy, *Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building A Healthy Information Environment 2* (2021), <https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf>.

FTC Chimes In

www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ▾ Policy ▾ Advice and Guidance ▾ News and Events ▾ About the FTC ▾

[Home](#) / [Policy](#) / [Advocacy and Research](#) / [Tech@FTC](#)

Tech@FTC

Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking

By: The FTC Office of Technology | March 16, 2023 | [f](#) [t](#) [in](#)



A deep dive into the technical side of FTC's recent cases on digital health platforms, GoodRx & BetterHelp

The Federal Trade Commission recently took enforcement action against GoodRx^[1] and BetterHelp^[2], two digital healthcare platforms, for allegedly sharing user health data with third parties for advertising. Both cases highlighted the use of third-party tracking pixels, which enable platforms to amass, analyze, and infer information about user activity.^[3] The remedies in GoodRx^[4] and BetterHelp^[5] include strong provisions like bans that place strict, comprehensive limits on whether and how certain user information may be disclosed for advertising. In GoodRx and BetterHelp, this included a ban on the sharing of health information for any advertising purposes, and the BetterHelp order further bans the disclosure of other personal information for re-targeting.

Subscribe

[Subscribe to Tech@FTC Blog updates](#)

Upcoming FTC Tech Events

Currently we have no upcoming Tech events. Please check back soon.

Additional Information

[Office of Technology Research & Investigation](#)

Categories

[Accountability](#) (2)
[Authentication](#) (1)
[Big data](#) (1)
[Cryptography](#) (1)
[Data security](#) (7)
[Privacy](#) (4)



FTC Enforcement

Home / News and Events / News / Press Releases

For Release

Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order

FTC says company disclosed user health data to third parties, deceived users about its data sharing practices and violated Health Breach Notification Rule

May 17, 2023 | [f](#) [t](#) [in](#)

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Health Care](#) | [Online Advertising and Marketing](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#) | [Tech](#) | [Health Privacy](#)

The Federal Trade Commission charged that the developer of the fertility app Premom deceived users by sharing their sensitive personal information with third parties, including two China-based firms, disclosed users' sensitive health data to AppsFlyer and Google, and failed to notify users about these unauthorized disclosures in violation of the Health Breach Notification Rule (HBNR).

"Premom broke its promises and compromised consumers' privacy," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "We will vigorously enforce the Health Breach Notification Rule to defend consumer's health data from exploitation. Companies collecting this information should be aware that the FTC will not tolerate health privacy abuses."

This is the FTC's second enforcement action involving the Health Breach Notification Rule following a settlement [announced in February](#) with telehealth and prescription drug discount provider GoodRx Holdings Inc. The FTC charged that GoodRx violated the rule by failing to notify users about the company's unauthorized disclosure of their personally identifiable health information to Facebook, Google and others.

Related Cases

[Easy Healthcare Corporation, U.S. v.](#)

For Consumers

Blog: [Pregnancy app Premom shared users' sensitive information](#)

[ftc.gov/yourprivacy](#)

For Businesses

Blog: [FTC says Premom shared users' highly sensitive reproductive health data: Can it get more personal than that?](#)

[Health Privacy](#)

Tags:

Home / News and Events / News / Press Releases

For Release

FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising

BetterHelp will be required to pay \$7.8 million for deceiving consumers after promising to keep sensitive personal data private, agency says

March 2, 2023 | [f](#) [t](#) [in](#)

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Health](#) | [Online Advertising and Marketing](#) | [Consumer Privacy](#) | [Health Privacy](#)

The Federal Trade Commission has issued a proposed order banning online counseling service BetterHelp, Inc. from sharing consumers' health data, including sensitive information about mental health challenges, for advertising. The proposed order also requires the company to pay \$7.8 million to consumers to settle charges that it revealed consumers' sensitive data with third parties such as Facebook and Snapchat for advertising after promising to keep such data private.

This is the first Commission action returning funds to consumers whose health data was compromised. In addition, the FTC's proposed order will ban BetterHelp from sharing consumers' personal information with certain third parties for re-targeting—the targeting of advertisements to consumers who previously had visited BetterHelp's website or used its app, including those who had not signed up for the company's counseling service. The proposed order also will limit the ways in which BetterHelp can share consumer data going forward.

"When a person struggling with mental health issues reaches out for help, they do so in a moment of vulnerability and with an expectation that professional counseling services will protect their privacy," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "Instead, BetterHelp betrayed consumers' most personal health information for profit. Let this proposed order be a stout reminder that the FTC will prioritize defending Americans' sensitive data from illegal exploitation."

Related Cases

[BetterHelp, Inc., In the Matter of](#)

Related actions

[BetterHelp, Inc.; Analysis of Proposed Consent Order To Aid Public Comment](#)

[Concurring Statement from Commissioner Wilson Regarding BetterHelp](#)

For Businesses

Blog: [FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises](#)

[Health Privacy](#)

Checklist: Identify & Evaluate

- ❑ Identify any/all third-party **data tracking technology** vendor(s)/suppliers.
- ❑ Identify all **applications or platforms** (e.g., EHR, web-based patient portals, websites, social media pages, mobile apps) where third-party data tracking technology **is enabled**.
- ❑ Identify **what specific data** (e.g., IP addresses, geographic location, home address, email, dates of appointments etc.) **is collected from/by such applications or platforms and for what purpose**.
- ❑ Identify exactly what specific **data is being/has been transmitted** to third-party data tracking technology vendor(s)/suppliers in connection with such data collection.
- ❑ Identify **the date(s)** on which each third-party data tracking technology vendor or supplier of web tracking services was first contracted/engaged by CE.
- ❑ Locate copies of each applicable service agreement(s) and **HIPAA BAAs** in place with third-party data tracking technology vendor(s) or supplier(s).
- ❑ Locate a copy of CE's **Security Evaluation** completed after third-party data tracking technology was implemented/enabled.
- ❑ Determine specifically whether any data collected/disclosed through third-party data tracking technology (such as **Google Analytics** or **Meta/Facebook Pixel**) included PHI.



Checklist: Assess & Respond **Security Incident or Breach?**

- ❑ If PHI was collected and disclosed through third-party data tracking technology, assess whether the disclosure constitute(s) a **Security Incident** or **Breach of Unsecured PHI**.
- ❑ Complete a **HIPAA Breach Risk Assessment** for every instance where unencrypted PHI was disclosed in an unauthorized manner due to implemented or enabled online tracking technologies which CE has discovered.
- ❑ Be prepared to describe/provide evidence of CE's investigation and, if applicable, **discovery of and response** to any Security Incident/Breach of Unsecured PHI to third-party data tracking technology vendors/suppliers, including investigative report, "Breach Risk Assessment," and corroborating documentation, such as access/activity logs, external investigative reports, forensic evaluations, reports from law enforcement, etc. Assess any state breach notification obligations which may be triggered in connection with the unauthorized disclosure of PHI.
- ❑ If a Breach of Unsecured PHI has occurred as a result of disclosure of PHI to third-party data tracking technology vendors or suppliers utilized by Covered Entity, **prepare, issue and document any Breach Notifications** in consultation with **insurance and legal counsel** to affected individuals and other required entities to the extent required by 45 C.F.R. §§ 164.404, 164.406 and 164.408.
- ❑ Be prepared to describe and provide evidence of **corrective/mitigating actions** taken in response to any Breach of PHI involving third-party data tracking technology vendors or suppliers of web tracking services (removal/disabling of tracking technologies, sanctions, revision of technical safeguards, policies or procedures, new policies/procedures, BAAs, termination of vendor, etc.



Checklist: Assess & Respond **Security Incident or Breach?** *(con't)*

- ❑ Be prepared to provide a **sample copy of any Breach Notification letter**(s) issued to affected individuals regarding the incident, including dates of notification.
- ❑ Be prepared to provide supporting documentation demonstrating that CE provided Notice to **prominent media outlet**(s) serving applicable State(s) or jurisdiction(s), if required.
- ❑ Be prepared to provide supporting documentation demonstrating that CE provided **Notice to HHS**, as required by §164.408.
- ❑ If CE did not issue notifications of the Breach(es), be prepared to provide **supporting documentation** of a Breach Risk Assessment completed in accordance with the Breach Notification Rule that concluded a Breach of Unsecured PHI was not likely to have occurred.



Checklist: Additional Considerations

- ❑ Identify and document the **Security Official** responsible for development/implementation of CE's policies/procedures required by the HIPAA Security Rule, and the **date** individual was designated.
- ❑ Describe and provide evidence of any mechanism CE has in place to **encrypt and decrypt ePHI**. Describe whether CE **encrypts data at-rest and in-transit** for web application(s), and include the **date** such encryption was implemented. If CE does not employ encryption methods for ePHI, provide dated documentation supporting **equivalent alternative safeguards**.
- ❑ Describe the **Security Awareness and Training** program implemented by CE.
- ❑ Documentation relating to CE's **Security Incident procedures, response and reporting** policies, and the policies it implements to **prevent, detect, contain, and correct** security violations.
- ❑ Identify CE's **most recent Risk Analysis**, as well as a copy of all Risk Analyses performed for or by Covered Entity within the past 6 years.
- ❑ Documentation demonstrating CE's **current policy/ies** regarding uses and disclosures of PHI **related to development and maintenance** of **websites, social media pages** (e.g., FaceBook), **patient portals**, and other **web-based platforms** in compliance with the HIPAA Privacy Rule.



Checklist: Mitigation

- ❑ **HIPAA BAA** is in place with the tracking technology vendor/supplier IF CE requires the data collected for its own Health Care Operation purposes.
- ❑ Require vendor/supplier **remove or disable** the tracking technology.
- ❑ If vendor/supplier unable to remove or disable the tracking technology, and will not sign a HIPAA BAA (or not appropriate i.e., not a business associate) consider the following options:
 - ❑ If feasible, **encrypt all ePHI** before it can be collected by the tracking technology.
 - ❑ **Implement a “pop-up” screen** requesting the user of any CE application or platform to digitally execute a fully compliant **HIPAA-compliant Authorization.**
- ❑ **Terminate** CE’s arrangement with a vendor/supplier if HIPAA BAA cannot be put in place, the tracking technology cannot be removed/disabled, ePHI cannot be encrypted and/or a HIPAA Authorization cannot be obtained in advance for the disclosures and purposes needed.
- ❑ **Polices to address tracking technologies:** (1) Development and maintenance of websites, social media pages (e.g., Facebook), patient portals and other web-based platforms in compliance with the HIPAA Privacy Rule, which includes steps CE takes to manage online tracking technologies in connection therewith; (2) Uses & Disclosures of PHI for Health Care Operations/Marketing/HIPAA Authorizations; (3) Uses & Disclosures to Business Associates pursuant to BA Contracts
- ❑ **Retrain workforce members**
- ❑ **Apply sanctions**



Be Proactive! Take Action!

- ***Assemble a “Task Force Team”***
 - IT Support
 - HIPAA Security Officer
 - Compliance
 - Vendor Representative
- ***Assess*** (it’s not just Meta Pixel)
 - Websites; FB Page; EMR Patient Portals; Mobile Applications
 - Google Analytics; Meta Pixel; other applications
 - Contract terms
- ***Address***
 - Reconfigure
 - Disable
 - Terminate

Compliance Checklist

CHECKLIST (CE)

Legal Health information eXchange

HIPAA Compliance Assessment & Mitigation for Enabled Online Tracking Technologies

Data Tracking Tech HIPAA Compliance Assessment

1. Identify and Evaluate Third-Party Data Tracking Technology.

- Identify any and all third party data tracking technology vendor(s) or suppliers of web tracking services used by Covered Entity.

[NOTE: In its December 2022 Guidance Bulletin, [HIEPA Online Tracking Technologies Guidance](#), OCR defined "tracking technology" as "a script or code on a website or mobile app used to gather information about users as they interact with a website or mobile app. Tracking technologies collect information in a variety of ways, including with cookies, web beacons or tracking pixels, session replay scripts, browser fingerprinting, and other means."

- Identify all of Covered Entity's applications or platforms (e.g., EHR, web-based patient portals, websites, social media pages, mobile apps) where third-party data tracking technology is enabled.

- Identify what specific data (e.g., including IP addresses and geographic location, as well as things like home address, email, dates of appointments etc.) is collected from or by such applications or platforms and for what purpose. Examples of purposes may include Covered Entity's health care operations (which are likely, permissible), or for other purposes, like marketing (which are likely, not permissible).

- Identify exactly what specific data is being/has been transmitted to the third party data tracking technology vendor(s) or suppliers of web tracking services in connection with such data collection.

- Identify the date(s) on which each third-party data tracking technology vendor or supplier of web tracking services was first contracted/engaged by Covered Entity. If Covered Entity did not specifically engage/contract the third-party data tracking technology vendor/supplier for web tracking services, identify the date(s) on which any such activities were nevertheless commenced by the vendor/supplier.

- Confirm whether data tracking technology is still being used or the date(s) it ended.

- Locate copies of each applicable service agreement(s) and HIPAA business associate agreement(s) in place with third-party data tracking technology vendor(s) or supplier(s) of web tracking services. Be prepared to provide evidence of how Covered Entity implements its policy and procedure requiring Business Associate Contracts to be put in place pursuant to 45 CFR § 164.308(b)(1). If an applicable service agreement(s) and/or HIPAA business associate agreement is not in place, confirm and document the reason(s) why and whether a HIPAA business associate agreement(s) is needed with the third party.

© 2025 Legal HIE Solutions LLC. All rights reserved.

DISCLAIMER: Do not rely on this tool to make any decision which requires the advice of an attorney. Last updated January 2025.

CHECKLIST (CE)

Legal Health information eXchange

HIPAA Compliance Assessment & Mitigation for Enabled Online Tracking Technologies

- Locate a copy of Covered Entity's Security Evaluation (required by 45 CFR 164.308(a)(8)) completed after third-party data tracking technology was implemented/enabled. Include information documenting the introduction of any tracking technologies that collect and/or transmit PHI to the tracking technology vendor(s) or supplier(s) of web tracking services (e.g., change request documents, approval emails). If none was previously conducted, conduct and document the performance of such Security Evaluation.

[NOTE: 45 C.F.R. § 164.308(a)(8) of the Security Rule contains the following Standard: "Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart."

- Determine whether any data collected and disclosed through third-party data tracking technology (such as Google Analytics or Meta/Facebook Pixel) included PHI. If the answer is yes, identify what PHI is or was disclosed, to whom, and the date(s) of disclosure(s). If the answer is no, document what data is or what disclosed, to whom, and why the information does not constitute PHI.

[NOTE: A determination of whether particular data constitute "Protected Health Information" is a [link](#), [discussing](#) determination which should be made in consultation with legal counsel and the compliance/privacy officer, particularly in light of the new December 2022 Guidance Bulletin issued by OCR and its expansive view of what constitutes "PHI". See [HIEPA Online Tracking Technologies Guidance](#).]

"Protected health information" means individually identifiable health information: (1) Except as provided in paragraph (2) of the definition, that is (A) Transmitted by electronic media; (B) Maintained in electronic media; or (C) Transmitted or maintained in any other form or medium. 45 C.F.R. § 160.103.

"Individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) That identifies the individual or (4) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

"Health information" means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. 45 C.F.R. § 160.102.

- Determine whether Covered Entity has received any notice(s), of which it is aware, from any other individual or entity, alleging that Covered Entity's use of tracking technologies is resulting in an impermissible disclosure of PHI. If so, identify the notification date(s), representative contacted, the name of the individual or entity that contacted Covered Entity, their contact information, and a short summary of what Covered Entity was told and how Covered Entity responded.

© 2025 Legal HIE Solutions LLC. All rights reserved.

DISCLAIMER: Do not rely on this tool to make any decision which requires the advice of an attorney. Last updated January 2025.

CHECKLIST (CE)

Legal Health information eXchange

HIPAA Compliance Assessment & Mitigation for Enabled Online Tracking Technologies

2. Assess Third-Party Data Tracking Activities for Potential Security Incident(s) and Breach(es) of Unsecured PHI.

- If PHI was collected and disclosed through third-party data tracking technology, assess whether the disclosure constitute(s) a Security Incident or Breach of Unsecured PHI, as defined by HIPAA.

[NOTE: A determination of whether a Security Incident or Breach of Unsecured PHI occurred is a [link](#), [discussing](#) determination which should be made in consultation with legal counsel and the compliance/privacy officer, particularly in light of the new December 2022 Guidance Bulletin issued by OCR and its expansive view of what constitutes "PHI". See [HIEPA Online Tracking Technologies Guidance](#).]

"Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. 45 C.F.R. § 164.402.

"Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 C.F.R. § 164.304.

"Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. 45 C.F.R. § 164.402.

Except as provided by 45 C.F.R. 164.402 (Exceptions to definition of breach), an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is [considered to be a breach](#) unless the covered entity or business associate, as applicable, demonstrates that there is a [low probability that the covered health information has been compromised based on a risk assessment](#) of at least the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the protected health information or to whom the disclosure was made;

(3) Whether the protected health information was actually acquired or viewed; and

(4) The extent to which the risk to the protected health information has been mitigated.

45 C.F.R. § 164.402

- Be prepared to describe in detail and provide evidence of Covered Entity's investigation and, if applicable, discovery of and response to any Security Incident or Breach of Unsecured PHI to third-party data tracking technology vendors or suppliers of web tracking services as required by 45 C.F.R. §§ 164.308(a)(6) (Security Incident Procedures) and 164.308(a)(1)(ii) (Security Management Process).

- Such evidence may include an investigative report and "Breach Risk Assessment" (see 45 C.F.R. § 164.402) created by or on behalf of Covered Entity upon discovery of a Breach as well as any corroborating documentation, such as access/activity logs, external investigative reports, forensic evaluations, reports from law enforcement, etc.

© 2025 Legal HIE Solutions LLC. All rights reserved.

DISCLAIMER: Do not rely on this tool to make any decision which requires the advice of an attorney. Last updated January 2025.

www.legalhie.com/membership



Connecting Healthcare with Legal Excellence SM

© 2023 Oscislowski LLC

Questions?



Attorneys at
Oscislawski LLC

Helen Oscislawski, Esq.

Principal, Attorneys at Oscislawski LLC

helen@oscislaw.com

609-835-0833



Need sample policies, tools and checklists
to help your organization comply with
Information Blocking Rules?

visit

www.legalhie.com/membership

Use Discount Code **NJHAJULY23** for a **\$250 discount**
on a Bronze, Silver or Gold **Organizational Plan**
subscription to access our compliance library!

EXPIRES December 31, 2023.