

Advertising Challenges in the Healthcare Context

How Healthcare Organizations Can Manage the Risks Presented by Online Ad Trackers & Pixels

Presented at the Privacy + Security Forum
Spring Academy

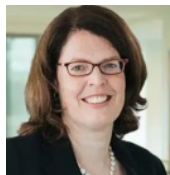


March 2023

With You Today...



Andrew Shaxted
Managing Director
FTI Consulting
andrew.shaxted@fticonsulting.com
+1 773 658 0241



Thora Johnson
Partner
Orrick, Herrington & Sutcliff LLP
thora.johnson@orrick.com
+1 202 339 8463



Sundeep Kapur
Senior Associate
Orrick, Herrington & Sutcliff LLP
Sundeep.kapur@orrick.com

Agenda

- Key Terms
- Setting the Stage
- Technical Overview of Tracker Functionality
- Marketing Under HIPAA
- OCR Guidance & Enforcement
- FTC Enforcement
- Litigation
- Consumer Perception
- Recommendations
- Other Emerging Issues

Key Technical Terms

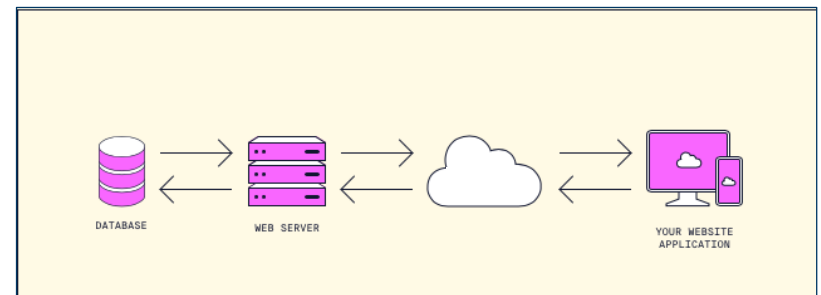
- An **Analytics Tracker** is a piece of code that is used to monitor and collect information concerning a user's interactions with a website, application, or other digital asset. This information can include website page views, clicks, web form entries, and other actions. Analytics trackers may also capture details about the user's device, the website the user is navigating from, and identifiable data elements such as: cookie identifiers, geo-location (with varying degrees of specificity), email address, phone number, first and last name, etc.
- A **Cookie** is a small piece of data that is stored on a user's device when they visit a website. Cookies can be used to store information about the user's preferences and browsing history, which can be accessed by the website later to provide a personalized experience.
- An **HTTP request** is a message sent by a client (such as a web browser) to a server, asking the server to perform a specific action or provide some information. HTTP requests are an essential part of the communication between web clients and servers, and they are used to request resources (such as web pages or images) or to submit data (such as a search query or a form submission).
- **Events** are typically used to track the performance of advertising campaigns, to measure the effectiveness of website or app features, or to understand users' behavior and preferences. For example, an event could be a user clicking on an ad, adding an item to their shopping cart, or signing up for a newsletter. Ad trackers typically allow advertisers to define custom events that are relevant to their business or goals, and to track these events in real time.
- A **Tracking Pixel ("Pixel")** is a type of analytics tracker. It is – in fact – a small transparent image that developers embed onto a web page. When the webpage loads (or some other pre-defined event occurs), the browser will send a GET request to the server asking for the Pixel image to load onto the page. This request for the Pixel contains parameters that provide information about the website, the specific page being viewed, information about the user's device, cookie values, and any other information the developer wishes to share.

Key Marketing & Advertising Terms

- An **Audience** refers to the group of users or customers who are being targeted by an ad campaign. An audience is typically defined by the advertiser based on various criteria, such as demographics, interests, behaviors, or location. For example, an advertiser may define their audience as "women aged 18-24 who are interested in fashion and who live in New York City".
- **Targeted ads** are ads that are tailored to the interests, preferences, and behavior of specific users or groups of users. These ads are delivered to users based on their past interactions with the website or app, or on other data that is available about them (such as their location, age, or gender). Targeted ads are typically more effective than non-targeted ads, as they are more relevant and engaging for the user.
- **Conversions** are the actions that advertisers consider valuable or desirable for their business or goals. Conversions are typically defined by the advertiser, and may include actions such as making a purchase, filling out a form, or subscribing to a newsletter. Advertisers use conversions to measure the success of their campaigns, and to optimize their ad delivery and targeting.
- **Attributions** are the process of assigning credit to the different touchpoints and channels that contribute to a conversion. Attributions are used to understand the user journey and to identify the most effective channels and tactics for driving conversions. Advertisers typically use attribution models to allocate credit to the different touchpoints, and to determine which channels are the most valuable for their business.

Webpage 101

- A web of HTML, CSS, and JavaScript, sent to you by the website host via the internet. The internet is made up of a bunch of resources hosted on different servers. The term “resource” corresponds to any entity on the web, including HTML files, stylesheets, images, videos, and scripts. To access content on the internet, your browser must ask these servers for the resources it wants, and then display these resources to you. This protocol of requests and responses enables you view *this* page in your browser.
- HTTP Requests: HTTP stands for Hypertext Transfer Protocol and is used to structure requests and responses over the internet. HTTP requires data to be transferred from one point to another over the network.
 - GET Requests: retrieve a specific resource from the web server. (“Hey, give me that image!”)
 - POST Requests: create a new resource on the web server (“Hey, take this webform data!”)
 - PUT Requests: update an existing resource (by id)
 - DELETE Requests: remove a specific resource (by id)
- Request Composition:
 - Path: the location of the resource expressed as a URL and sub-path (Letter Analogy: the address on the front of the envelope)
 - Header: allows the client to pass along information about the request (Letter Analogy: instructions like “certified mail” or “return receipt requested”)
 - Body: message containing data (Letter Analogy: the letter in the envelope)



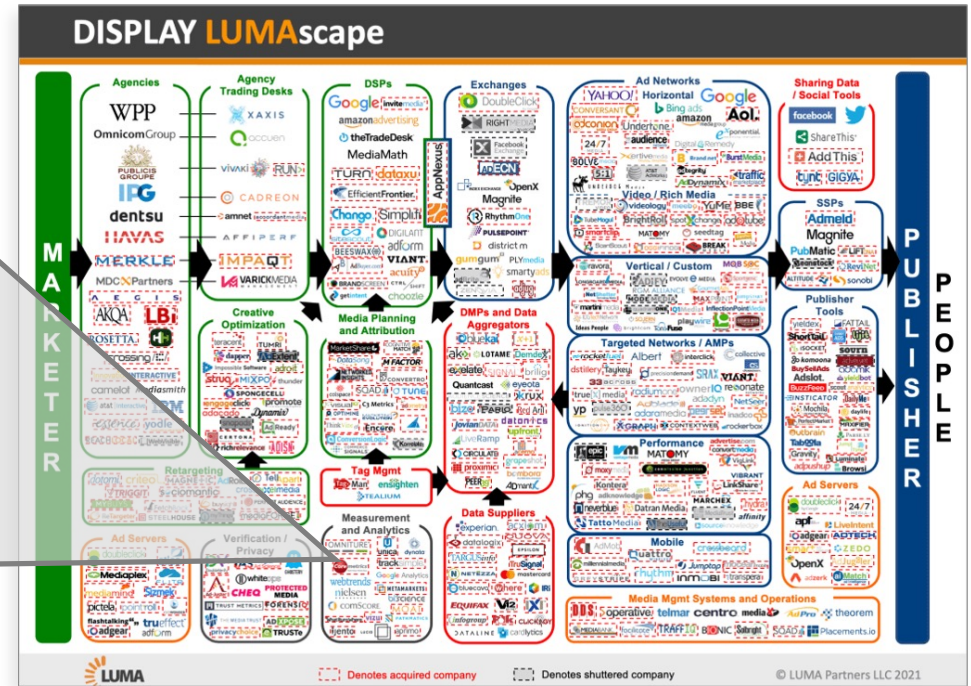
Setting the stage

Analytics Trackers are One Small Piece of the Advertising Puzzle



- Not all trackers are built to do the same thing.
- There are hundreds (even thousands) of analytics trackers available on the market today, serving various needs.

Core Analytics Trackers	Social Media Trackers	Screen Recording/Heat Mapping	A/B Testing	Other Specialized Trackers
<ul style="list-style-type: none"> • Google Analytics • Adobe Analytics 	<ul style="list-style-type: none"> • The Meta Pixel • The SnapChat Pixel • The Tik Tok Pixel • The Pinterest Tracker • Twitter Tracker 	<ul style="list-style-type: none"> • Hotjar • Fullstory • Mouseflow • Crazy Egg 	<ul style="list-style-type: none"> • Optimizely • AB TASTY • VWO 	<ul style="list-style-type: none"> • Adobe Analytics for Streaming • Data.ai (F.K.A. App Annie) Mobile Analytics • Hotjar (Heatmapping and screen recording)



Setting The Stage – The Meta Pixel

Representative Functionality of Analytics Trackers & Pixels



Base Code

E.g. Meta Pixel Base Code Deployed via Google Tag Manager

```
Tag Configuration
Tag Type
Custom HTML
Custom HTML Tag
HTML
1 <!-- Facebook Pixel Code -->
2 <script>
3 !function(f,b,e,v,n,t,s)
4 {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
5 n.callMethod.apply(n,arguments):n.queue.push(arguments)};
6 if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
7 n.queue=[];t=b.createElement(t);t.async=!0;
8 t.src=v;s=b.getElementsByTagName(e)[0];
9 s.parentNode.insertBefore(t,s)}(window, document,'script',
10 'https://connect.facebook.net/en_US/fbevents.js');
11 fbq('dataProcessingOptions', ['LDU'], 0, 0);
12 fbq('init', '1205071633604892');
13 fbq('track', 'PageView');
14 </script>
15 <noscript></noscript>
18 <!-- End Facebook Pixel Code -->
```

Dashboard-based no-code configuration.

E.g. Automatic Advanced Matching Settings in Meta Pixel Dashboard

Turn on automatic advanced matching
Use customer information to match event instances on your website to a Facebook account. This helps us show relevant ads to people on Facebook. [Learn more](#)

Automatic advanced matching ON

Hide options

Email ON

Gender ON

City, state, ZIP code and country ON

First and last name ON

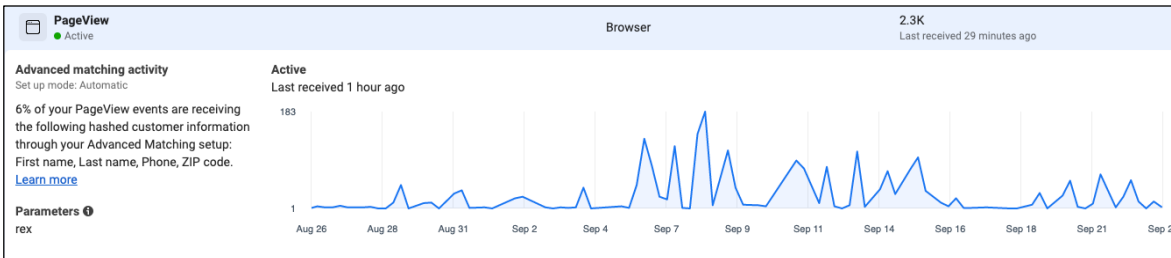
Phone number ON

Date of birth OFF

External id OFF

Analytics Dashboard

E.g. Meta Pixel Dashboard



Representative Functionality of Social Media Analytics Trackers – The “Meta Pixel”

Not (always) a black box...

A **Tracking Pixel** (“Pixel”) is a type of analytics tracker. It is – in fact – a small transparent image that developers embed onto a web page. When the webpage loads (or some other pre-defined event occurs), the browser will send a GET request to the server asking for the Pixel image to load onto the page. This request for the Pixel contains parameters that provide information about the website, the specific page being viewed, information about the user’s device, cookie values, and any other information the developer wishes to share.

Request Details

Request Details

Sizes (1.7 kB)

www.facebook.com/tr/?id=90340759...

Request Headers (1.3 kB) Request Body (0 B) Response Headers (357 B) Response Body (0 B)

Statistics

Request Details

Url	www.facebook.com/tr/?id=9034...&ev=Booking%2...
Method	GET
Client IP	127.0.0.1
Remote IP	31.13.71.36
Protocol	https
SSL Version	None

Corresponding Cookies Sent with the Request

Name	Value
sb	WnIXY_7NTwKvEVUdqAijGpQ
datr	XHIXY-1F0z60Ro32L3RRCUwd
c_user	100085046944794
xs	49%3AshNOi2fUYgo0Vw%3A2%3A1662481002%3A-1%3A-...
fr	0ukUkzN3gmHHgXrvB.AWU_h1fC-qONaljh3ILD2RBTAZI.BjJ...

Request

https://www.facebook.com/tr/?id=903... HTTP/1.1 GET

Headers (14) Params (19) Cookies (7) Raw Body

Key	Value
id	90340
ev	Booking Widget Touch Email
dl	https://www.../book-online/
rl	https://
if	false
ts	1671501585344
cd[name]	email
cd[email]	chris.jones@mail.com
cd[url]	https://www.../book-online/
cd[path]	/book-online...
cd[isIosPwa]	false
cd[isAndroidPwa]	false
cd[isIosApp]	false
cd[isAndroidApp]	false
cd[isNativeApp]	false
cd[originalEventName]	Booking Widget- Touch Email
sw	1280
sh	720

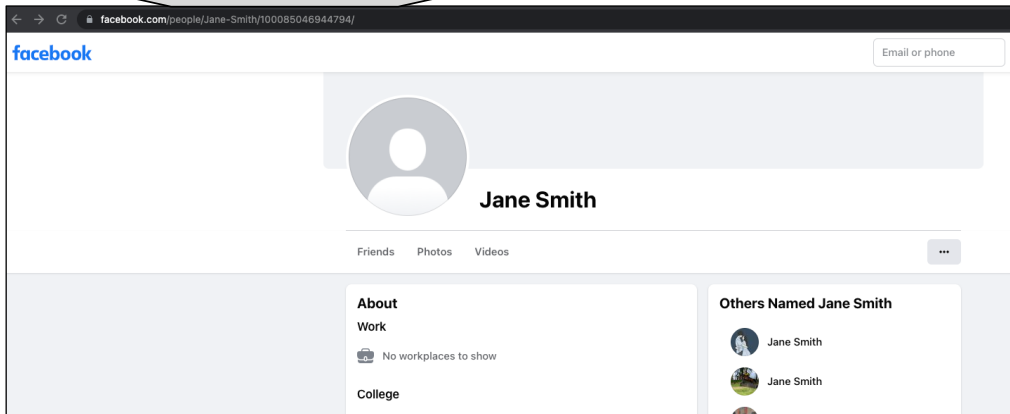
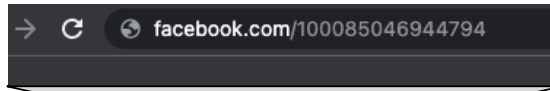
Setting the stage

Representative Functionality of Social Media Analytics Trackers – The “Meta Pixel”

Corresponding Cookies Sent with the Request

Name	Value
sb	WnlXY_7NTwkVgEVUdqAijGpQ
datr	XHIXY-1F0z60Ro32L3RRUwd
c_user	100085046944794
xs	49%3AshNOI2fUYgo0Vw%3A2%3A1662481002%3A-1%3A-...
fr	0ukUkzN3gmHHgXrvB.AWU_h1fc-qONalj3ILD2RBTazI.BjJj...

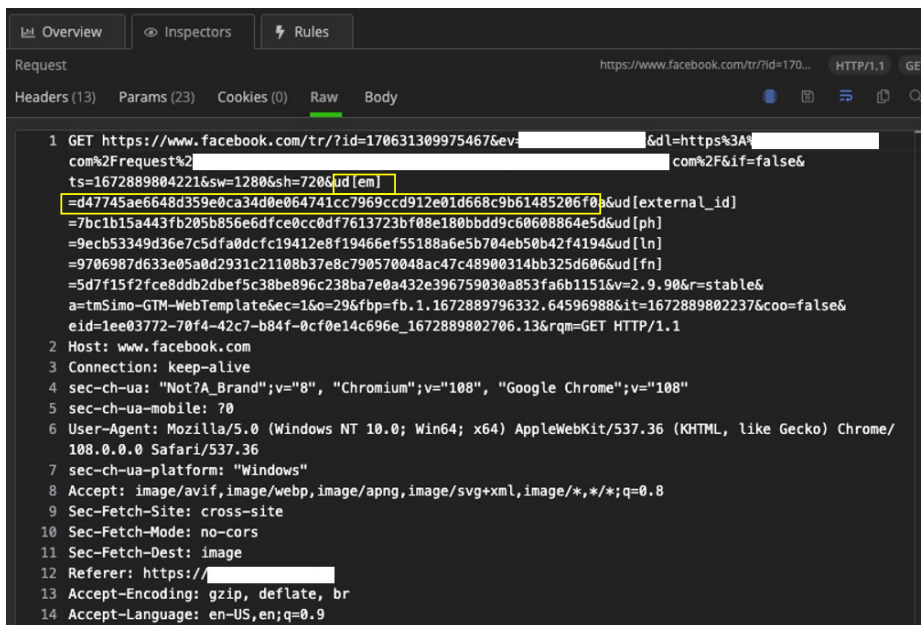
c_user Cookie value belonging to FTI’s test user “Jane Smith” appended to Facebook URL.



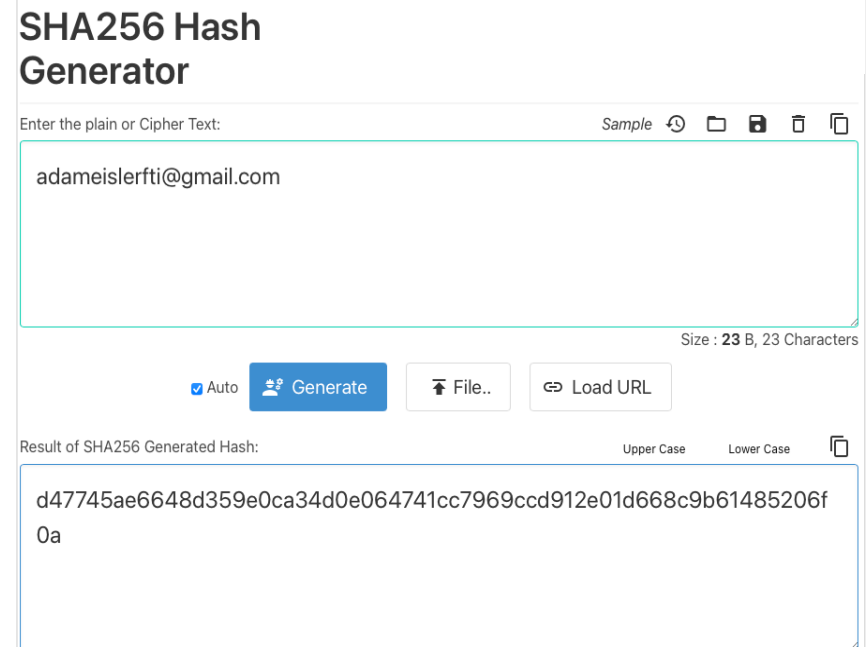
Setting the stage

Representative Functionality of Analytics Trackers & Pixels – The “Meta Pixel”

Advanced Matching is a feature used in analytics trackers to collect additional information about website visitors, such as email addresses or user IDs. This information is then used to link user data across different platforms and devices, allowing for more accurate tracking and reporting of user behavior.



```
1 GET https://www.facebook.com/tr/?id=170631309975467&ev=[redacted]&sd=https%3A%3A[redacted]
com%2Frequest%2F[redacted]&com%2Fif=false&
ts=1672889804221&sw=1280&sh=720&[redacted]
=d47745ae6648d359e0ca34d0e064741cc7969ccd912e01d668c9b61485206f0[redacted]
=7bc1b15a443fb205b856e6dfce0cc0df7613723bf08e180bbdd9c60608864e5d&ud[ph]
=9ecb53349d36e7c5dfa0dcfc19412e8f19466ef55188a6e5b704eb50b42f4194&ud[ln]
=9706987d633e05a0d2931c21108b37e8c790570048ac47c48900314bb325d606&ud[fn]
=5d7f15f2fce8ddb2dbef5c38be896c238ba7e0a432e396759030a853fa6b1151&v=2.9.90&r=stable&
a=tmSimo-GTM-WebTemplate&ec=1&o=29&fbp=fb.1.1672889796332.64596988&it=1672889802237&coo=false&
eid=1ee03772-70f4-42c7-b84f-0cf0e14c696e_1672889802706.13&rqm=GET HTTP/1.1
2 Host: www.facebook.com
3 Connection: keep-alive
4 sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
108.0.0.0 Safari/537.36
7 sec-ch-ua-platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://[redacted]
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
```



SHA256 Hash Generator

Enter the plain or Cipher Text: Sample 🔄 📄 🔒 🗑️ 📋

adameislerfti@gmail.com

Size : 23 B, 23 Characters

Auto Generate

Result of SHA256 Generated Hash: Upper Case Lower Case 📋

d47745ae6648d359e0ca34d0e064741cc7969ccd912e01d668c9b61485206f0a

Legal Overview

"Marketing" Under HIPAA

- General Rule: Entity must obtain a written HIPAA authorization from the patient before using or disclosing a patient's PHI for marketing.

- Marketing means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." 45 C.F.R. 164.501

- Except where the provider receives financial remuneration for making the communication, marketing does **not** mean a communication made:
 - For treatment of an individual by a health care provider;
 - To describe a health-related product or service provided by the covered entity making the communication;
 - For case management and care coordination;
 - To direct or recommend alternate treatments, therapies, providers, or settings of care.

"Marketing" Under HIPAA

- In practice, the following activities are permitted without a written HIPAA authorization:
 - Marketing CE's *own* products and services;
 - Sharing general healthcare news relevant to CE's patients or enrollees;
 - Contacting an individual to schedule treatment;
 - Sharing information about new treatments.

- The following activities are prohibited without a written HIPAA authorization:
 - Marketing a third party's product or service (like a third-party health app);
 - Sharing a patient list with a third party for that party to market its own product or service;
 - Using patient names or identifying information in marketing materials.

OCR Guidance on the Use of Tracking Technologies

- In December 2022, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued guidance on the use of third-party cookies, pixels, and other tracking technologies by entities subject to HIPAA.

- According to OCR, when a third-party tracking technology used on an entity's website or mobile app has access to PHI, the disclosure is subject to HIPAA and is prohibited without a business associate agreement or a written HIPAA authorization.
 - OCR broadly defines PHI to include IP address, medical device IDs, geographic location, advertising IDs, and any other unique identifying code.
 - According to OCR, this information is PHI even the information does not include specific treatment or medical billing information or if the individual does not have an existing relationship with the entity.
 - Why? "Indicative that the individual has received or will receive health care services or benefits from the covered entity."

OCR Guidance (continued)

- **User-Authenticated Web Pages:** In general, if a user has authenticated into a site (like a patient portal), HIPAA will apply because tracking technologies will have access to PHI.

- **Unauthenticated Web Pages:** No issue *unless* the tracking vendor has access to PHI. HIPAA may still apply to the following unauthenticated web pages:
 - Web pages that include a login for a patient portal or a user registration page;
 - Web pages that permit individuals to search for doctors or schedule appointments; or
 - Web pages that address specific symptoms or health conditions.

- **Mobile Health Applications:**
 - HIPAA applies if the app is offered by a HIPAA-covered entity or business associate *and* the tracking technology vendor collects PHI.
 - HIPAA does not apply if the app is direct-to-consumer.

- Note that an update to the HIPAA Privacy Rule is expected to be published in March 2023, which may address this guidance in more detail.

Potential HIPAA Liability

- The Office for Civil Rights ("OCR") in the Department of Health and Human Services is responsible for enforcing HIPAA.

- Entities that violate HIPAA may be subject to non-punitive measures, such as voluntary compliance or technical adjustments. However, OCR may also issue the following financial penalties:
 - **Tier 1:** Violation that the covered entity was unaware of and could not have realistically avoided. *Fine range is \$127 - \$60,973 per violation.*
 - **Tier 2:** Violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. *Fine range is \$1,280 - \$60,973 per violation.*
 - **Tier 3:** Violation as a direct result of "willful neglect" of HIPAA in cases where an attempt has been made to correct the violation. *Fine range is \$12,794 - \$60,973 per violation.*
 - **Tier 4:** Violation constituting "willful neglect" of HIPAA where no attempt has been made to correct the violation within 30 days. *Minimum fine is \$60,973 per violation.**

* Note that the penalty amounts will increase when the HHS publishes the inflation adjustment multiplier for 2023.

And It Is Not Just Covered Entities

- The FTC took enforcement action against GoodRx Holdings for failing to notify consumers of unauthorized disclosures of personal health information to: Facebook, Google, Criteo and others.

- The Order requires GoodRX to:
 - Is permanently prohibited from disclosing user health information with applicable third parties for advertising purposes.
 - Must obtain users' affirmative express consent before disclosing user health information with applicable third parties for other purposes.
 - Must pay a \$1.5 million penalty.

- The FTC has requested comments on commercial surveillance.

Healthcare Pixel Litigation Themes

- Since June 2022, **40+** class action lawsuits have been filed against hospitals and healthcare companies nationally for their use of tracking technologies.
- While most cases are still in the early stages, a suit filed in Massachusetts settled for **\$18.4 million** in early 2022 (before OCR released its guidance).

Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for \$18.4 Million

Posted By HIPAA Journal on Jan 20, 2022

HEALTH CARE

STAT+

UPMC, Advocate Aurora, Duke fighting lawsuits over use of Meta's tracking tool

August 11, 2022 04:01 PM

Lawsuit alleges Northwestern Memorial gave sensitive patient data to Facebook's parent

Similar lawsuits have recently been filed against hospitals across the country, alleging that providers and Meta violated privacy laws.

Healthcare Pixel Litigation Top 10 Claims

1. Violation of State Health Records Laws (like the Confidentiality of Medical Information Act)
2. Violation of Federal and State Wiretap Acts (like the California Invasion of Privacy Act or the Electronic Communications Privacy Act)
3. Violation of State Unfair or Deceptive Acts and Practices ("UDAP") Laws
4. Video Privacy Protection Act
5. Violation of State Unfair Competition Law
6. Intrusion Upon Seclusion – Invasion of Privacy (including under the California Constitution)
7. Unjust Enrichment
8. Breach of Contract/Implied Contract
9. Breach of Fiduciary Duty
10. Negligence

Potential Statutory Liability

■ California Confidentiality of Medical Information Act ("CMIA")

- Damages if Disclosure Led to Economic Loss or Personal Injury*: Compensatory damages, punitive damages up to \$3,000 and attorneys' fees not to exceed \$1,000, and costs of litigation for any violating disclosure of medical information that resulted in economic loss or personal injury to the patient.
- Damages for Negligent Disclosures*: Nominal damages of \$1,000 per violation, and actual damages, if any, for any negligent disclosure of medical information.

■ California Invasion of Privacy Act ("CIPA")

- Damages*: \$5,000 per violation or three times actual damages, if any.

■ Electronic Communications Privacy Act ("ECPA")

- Damages*: The greater of: (i) the sum of actual damages suffered by the individual and profits made by the violator as a result of the violation; or (ii) statutory damages of \$100/day for each day of the violation or \$10,000, whichever is greater, per person.

Consumer Perceptions and Pixel Usage

- In June 2022, *The Markup* published an article alleging that many hospital websites sent sensitive medical information to Facebook via the Meta Pixel without authorization.
- According to the article, 33 of the top 100 hospitals in the United States used the Meta Pixel on their websites.
- After the article was published, a flood of consumer class action claims were filed against hospitals for their use of tracking technologies on their websites and mobile apps.

The Markup

Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

Solutions – How to Think About Marketing/Advertising

- Comprehensive **governance program** to manage, monitor, and support the implementation of third-party tracking tool usage.
- Hypothetically, **obtain HIPAA-compliant patient authorization** to disclose PHI with third-party tracking technology vendors. Note that a website cookie banner is not sufficient.
- For analytics providers, **enter into a business associate agreement** ("BAA"), where possible, prior to placing an analytics tool on your website.
- Identify and separate pages that capture PHI from those that do not. **Only use tracking tools on pages where PHI is not captured** unless you've entered into a BAA with the vendor or received a written HIPAA authorization.
- Where possible, **build and use internal technologies** for analytics instead of technology from a third-party vendor (with effective oversight by the governance program).
- Take steps to **de-identify any identifying information** (including IP address) before it is sent to third-party vendors.
- Retargeting is a high-risk option when leveraging data collected from patient-facing sites under the HIPAA guidance. Instead, **purchase vetted and aggregated third-party marketing segments** to market your products and services to the right audience.

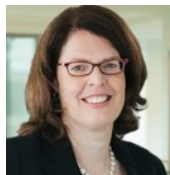
Related Emerging Issues – Session Replay and Chatbots

- **Session Replay.** A session replay code enables website operators to record and replay user interactions with their websites, including clicks, scrolls, hovers, web pages visited, and data submissions. This information is often used for marketing purposes. Session replay has been the subject of recent state wiretap law litigation.
- **Chatbots.** Websites use chatbots to respond to user questions about companies and their services, and the chatbots may retain transcripts of the communications. Individuals are suing companies that use this technology, alleging that it is a violation of wiretapping laws.

Contact Information



Andrew Shaxted
Managing Director
FTI Consulting
andrew.shaxted@fticonsulting.com
+1 773 658 0241



Thora Johnson
Partner
Orrick, Herrington & Sutcliff LLP
thora.johnson@orrick.com
+1 202 339 8463



Sundeep Kapur
Senior Associate
Orrick, Herrington & Sutcliff LLP
Sundeep.kapur@orrick.com