K&L GATES

Ad Tracking Tech in Health Care: The Current Regulatory and Litigation Landscape for HIPAA-Regulated Entities

Jake Bernstein, Gina Bertolini, Michael J. Stortz

Overview

- Understanding the Technology
  - Social media pixels; tracking cookies
  - How and what data is disclosed
  - Third party use
- Regulatory Activity
  - OCR Guidance
  - FTC Enforcement
  - Joint OCR-FTC Letter
  - AHA Letter to OCR
- Litigation update
  - ND Cal decisions
- Take-aways

Introduction to Ad Trackers

Online Ad Tracking Technologies 201

- **Cookie:** a small text file installed on a user's client (web browser usually, which means computer storage)
- **Pixel:** originally, a 1x1 transparent jpeg file, but now also lines of Javascript or other code (a *beacon* is a variant)
- **Tracking URL:** a (often *very long)* web address that transmits a significant amount of data directly within the "link" that is read by a receiving website
- **IP Address:** a computer's network location expressed either in IPv4 or IPv6 forming critical part of TCP/IP (Transmission Control Protocol/Internet Protocol)
- **Device Fingerprint:** unique set of characteristics of any given device (IP Address, OS, browser, etc.)

Online Ad Tracking Technologies 201

- **Tracking** combines Cookies, Pixels, Tracking URLs and Device Fingerprint with the immense computing power of modern databases to trace and record online activity across the internet
  - Normal URL: https://www.awebsite/a-landing-page/
  - Tracking URL: https://www.awebsite/a-landing-page/?utm_campaign=newsletter-campaign&utm_source=email
    - Encoded in this URL is information that you arrived at the landing page from a newsletter campaign sent via email
    - This information is stored and used to optimize future campaigns
- **Ad Tracking** is fundamentally about tracking performance of online ads so money is spent where it does the most good (for the advertiser).
  - **Two key terms**: Advertiser is the entity trying to sell something. Publisher is the entity where the advertisement appears.

The Meta Pixel

The Code

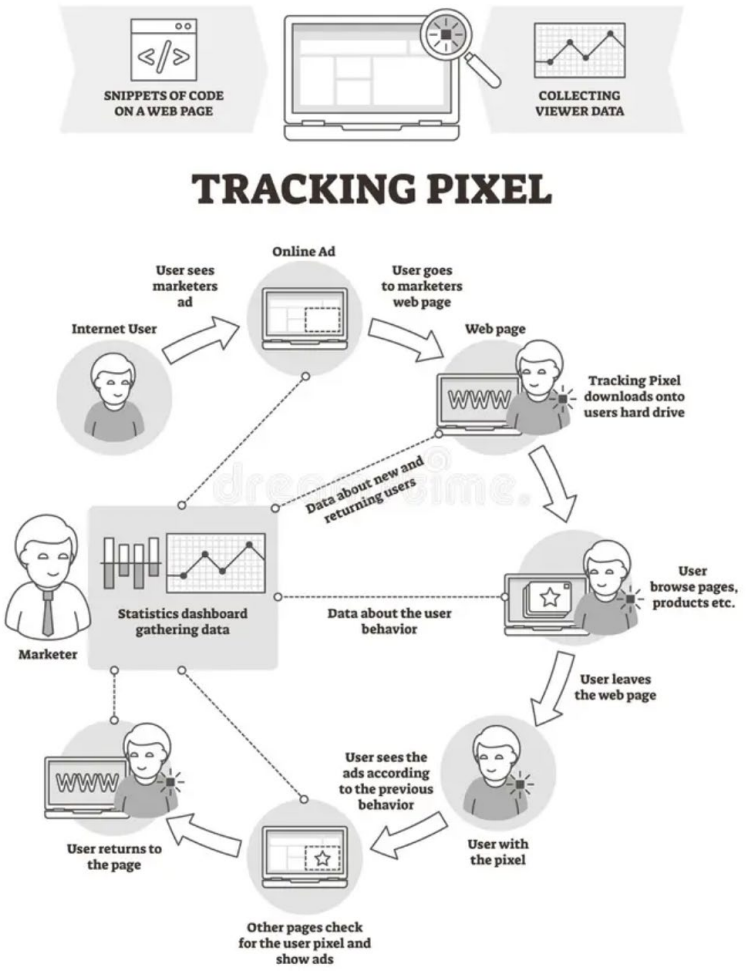
The Pixel

```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '{your-pixel-id-goes-here}');
  fbq('track', 'PageView');
</script>
<noscript>
  <img height="1" width="1" style="display:none"
       src="https://www.facebook.com/tr?id={your-pixel-id-goes-here}&ev=PageView&noscript=1"/>
</noscript>
<!-- End Facebook Pixel Code -->
```

- This is JavaScript, which is the scripting language upon which the modern web is built (along with several others).
- The “pixel” evolved from a relatively simple tracker that sent a ping on page load to the JavaScript- and HTML-powered surveillance mechanisms of today

Code from https://developers.facebook.com/docs/meta-pixel/get-started (really)

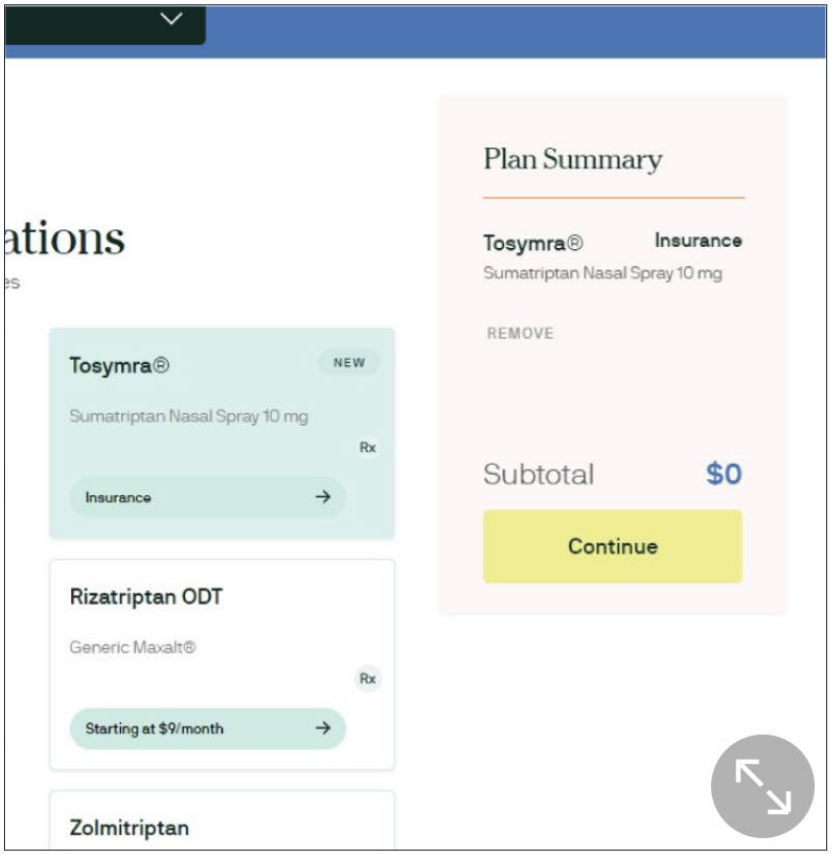
The Tracking Pixel Cycle

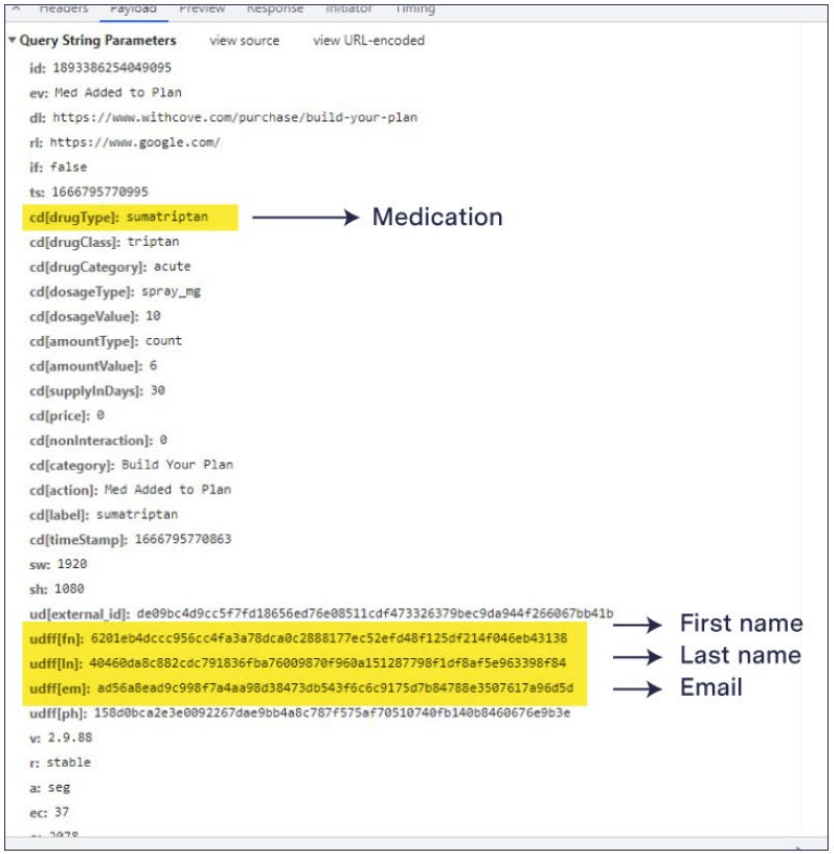


- Meta Pixel collects data on website visitors independently of Facebook or Instagram accounts
- For Facebook users logged in on any given browser, additional third-party cookies are used to create an expansive tracking network
- Advanced Matching Parameters
  - Allows Meta to connect collected event data to users, with or without Facebook's browsers cookies
  - Available to help target ads
- See How We Built a Meta Pixel Inspector – The Markup for more details

From www.dreamstime.com (royalty free)

Using the Meta Pixel for Health Data





Hashing ≠ Deidentified

Meta's Advanced Matching allows it to take hashed data and match it up with known user accounts.

Source: [Facebook Is Receiving Sensitive Medical Information from Hospital Websites – The Markup]

Meta Pixel and PHI Collection

Meta Pixel *is* installed on patient portals

Example of how Meta Pixel can transmit *obviously* sensitive information back to Facebook.

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

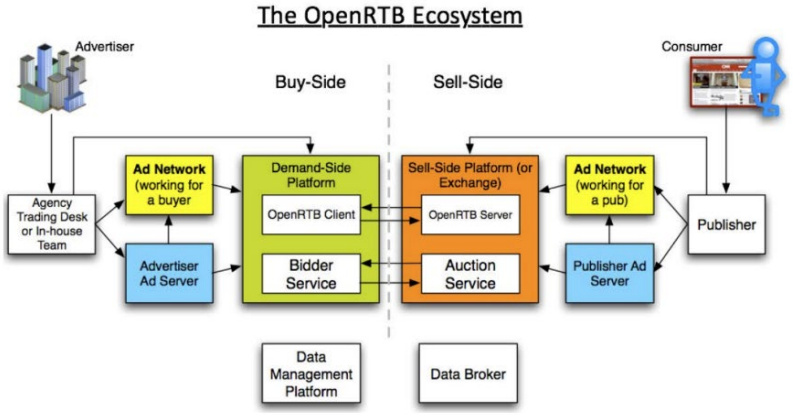
The Meta Pixel installed on [redacted] Healthcare's MyChart portal sent Facebook details about a real patient's upcoming doctor's appointment, including date, time, the patient's name, and the name of their doctor

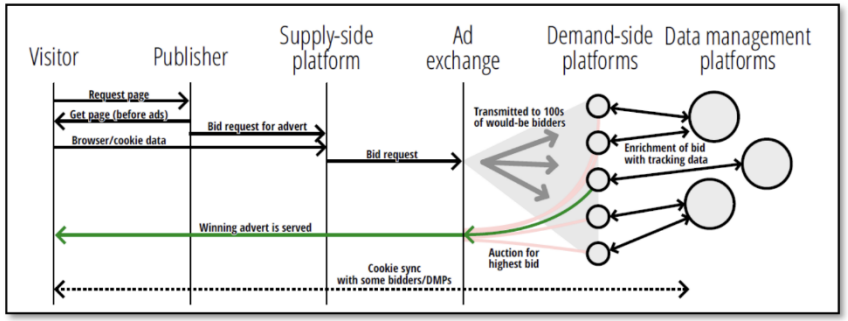
1. Patient name
2. Date and time of appointment
3. Name of provider


```
{"classList":"_Link+_actionable+_link+_readOnlyText+_InternalLink+main","destination":"https://mychart.[redacted]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[redacted]rg, Mozilla Rally

Complexity of the Ad Tech Ecosystem





Diagrams underscore the sheer complexity of online ad tracking "consent" systems.

IAB Europe's "Transparency & Consent Framework" invalidated by Belgian Data Protection Authority in February 2022

Ad Trackers:

Legal and Regulatory Considerations

Uses of Tracking Technologies by Health Care Entities

- Companies can use information obtained:
  - to help improve patient care or user experience of the website or app
  - to assist entities with online advertising
- Use for advertising purposes requires entities to disclose information obtained by tracking technologies to third parties, such as Meta and Google
- Is information obtained by health care provider entities protected by HIPAA?
  - If so, information cannot be disclosed for marketing purposes without a HIPAA-compliant authorization
  - Other federal laws, such as 42 CFR Part 2 (Confidentiality of Substance Use Disorder Records) may apply

Uses of Tracking Technologies by Health Care Entities

- Protected Health Information ("PHI")
  - information that identifies an individual, or for which there is a reasonable basis to believe the information can be used to identify an individual
  - that is created or received by a health care provider, health plan, or health care clearinghouse
  - that relates to (i) the past, present, or future physical or mental health or condition of an individual, (ii) the provision of health care to an individual, or (iii) the past, present, or future payment for the provision of health care to an individual
  - 45 CFR 160.103 (eCFR :: 45 CFR Part 160 -- General Administrative Requirements)

"Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" – OCR Bulletin, 12/2022

- Guidance released by Health and Human Services' Office for Civil Rights (OCR) - December of 2022
- Issued due to the proliferation of tracking technology tools on health-related websites and mobile apps, including entities regulated by HIPAA (e.g., health care providers that are Covered Entities and their Business Associates)
- Helps identify whether information shared through the use of tracking technologies is PHI
- Available at HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information | HHS.gov

OCR Guidance on Online Tracking Technologies

- Primarily addresses the use of online tracking technology by HIPAA "regulated entities" (i.e., Covered Entities and Business Associates)
- OCR expressed the position that identifiable information received by a HIPAA regulated entity's website or mobile application "generally is PHI"
  - even if the individual does not have an existing relationship with the entity
  - even if the information does not include specific treatment or billing information like dates and types of health care services
  - Reasoning: this information is indicative that the individual has received or will receive health care services or benefits from the entity and "relates to the individual's past, present, or future health or health care or payment for care."

OCR Guidance on Online Tracking Technologies

OCR identifies three online environments in which tracking technology is used:

1) user-authenticated web pages
2) unauthenticated web pages
3) mobile apps

OCR Guidance on Online Tracking Technologies

Online Environments Using Tracking Technologies	Examples	Information Collected	PHI?
User-authenticated web pages	Patient portals, telehealth platforms (log-in required)	IP address; MRN; home or email addresses; dates of appointments; diagnosis, treatment, billing, & Rx information	Tracking technologies will have access to PHI; HIPAA-compliant authorization for marketing uses or disclosures and BAA are required
Mobile apps	Mobile apps offered by HIPAA regulated entities (generally requires log-in, but not necessarily)	Information typed or uploaded into the app; information provided by the app user's device (e.g., fingerprints, network location, geolocation, device ID, advertising ID)	Tracking technologies will have access to PHI; HIPAA-compliant authorization for marketing uses or disclosures and BAA are required

OCR Guidance on Online Tracking Technologies

Online Environments Using Tracking Technologies	Examples	Information Collected	PHI?
Unauthenticated web pages	General information web pages of HIPAA regulated entities (e.g., location, services, policies and procedures) (no log-in required)	IP address, information regarding the user's movements, including information typed in (for example, to search a particular condition, health care provider, location, etc.)	Tracking technologies *may* have access to PHI, depending on the information searched • creation of log-in for patient portal or user-registered web page are done on an unauthenticated webpage b/c the user does not yet have access credential • navigating to symptom or condition specific pages • searching for health care providers or scheduling appointments HIPAA-compliant authorization for marketing uses or disclosures and BAA *may be* required

OCR Guidance on Online Tracking Technologies

- OCR Guidance not entirely clear regarding searches for symptom or disease-specific conditions on unauthenticated websites
  - Examples provided relate to searching for health care providers or scheduling appointments
  - OCR does not provide any examples referencing a search for specific conditions or symptoms
  - A person could search a website for specific health conditions or symptoms for many reasons unrelated to their own health care (e.g., looking for a family member, friend, or coworker; researching a health condition or symptom for work or school; curiosity regarding a particular condition or symptom)

American Hospital Association (AHA) Letter to OCR

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(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.

American Hospital Association (AHA) Letter to OCR (05/22/23)

- AHA provided comments to OCR related to the reproductive health care NPRM and urged OCR to suspend or amend its Tracking Technologies Guidance (https://www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance)
  - AHA expressed support for reproductive health care privacy: proposed rule's heightened privacy protections enhance provider-patient relationships
  - As part of that letter, AHA requested OCR to reconsider whether its ad tracking guidance is necessary "in light of heightened privacy protections" in the NPRM, citing that OCR's Dec. 2022 guidance was motivated, at least in part, by the desire to protect reproductive health information
  - Alternatively, if OCR maintains its Dec. 2022 guidance, AHA requested that OCR amend it "to better reflect the realities of online activity by hospitals and health systems"

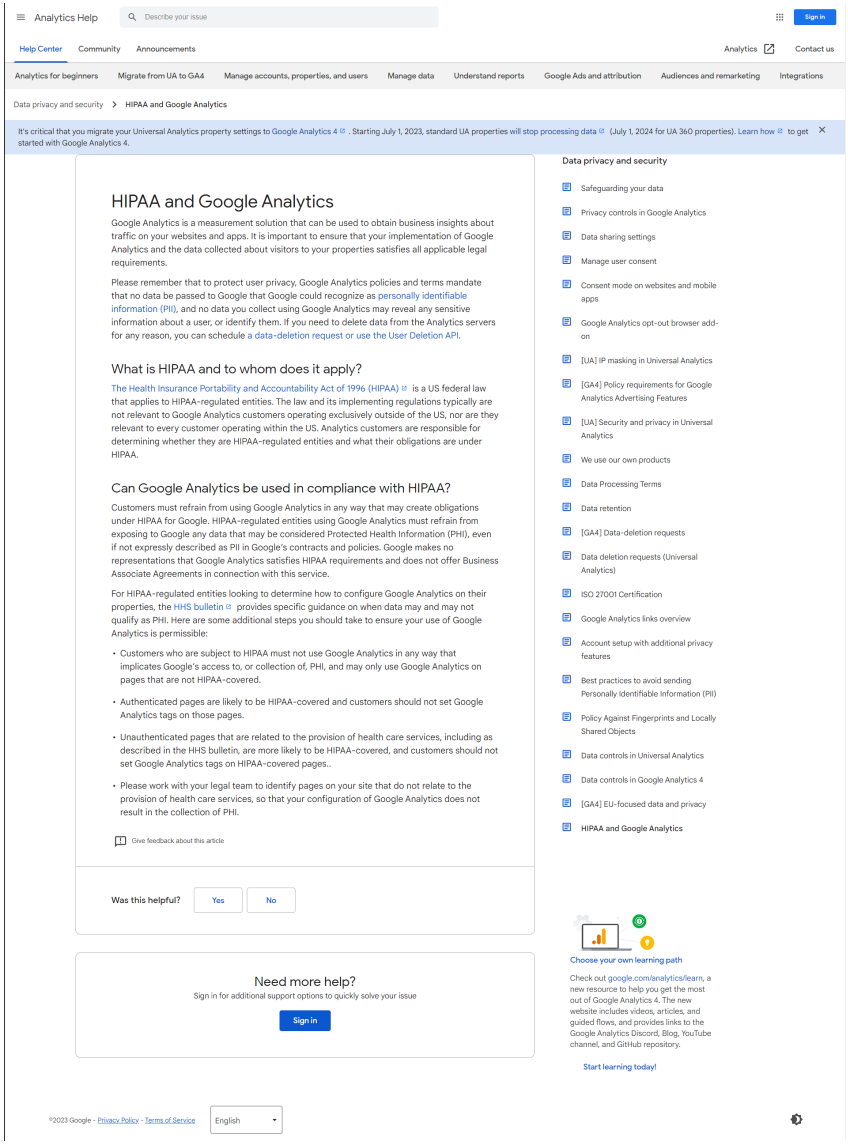
American Hospital Association (AHA) Letter to OCR

- IP address is "simply a long string of numbers assigned to every device connected to a network that uses the internet""
- "Health misinformation" is a serious threat to public health, and limiting the spread of health misinformation is a "moral and civic imperative" (referencing a 2021 report by U.S. Surgeon General Murthy)
  - Hospitals and health systems play an important part in providing consumers accurate, trustworthy, and helpful resources
  - AHA's members reach underserved populations that "would not otherwise have access to reliable health information"
- Treating all IP addresses as PHI is too broad
  - will ***reduce*** public access to credible information
  - will have "significant adverse consequences" to hospitals, patients, and the public
  - does not take into account context and whether someone is seeking health care or "just a curious online visitor"

American Hospital Association (AHA) Letter to OCR

- Third party vendors not subject to HIPAA
  - Generally make no representations that they will comply with HIPAA
  - Will not sign Business Associate Agreements (BAAs)
- Hospitals are in the middle, OCR Guidance subjects them to enforcement, class-action lawsuits, loss of millions of dollars in investments in websites, portals, and apps
- AHA requests
  1) Suspend Guidance
  2) Alternatively, amend Guidance such that IP addresses alone are not unique identifiers, OR if they are, only on authenticated webpages (e.g., patient portals)
  3) If unwilling to do the above, seek comment via RFI and notice-and-comment rulemaking
  4) Coordinate with Federal Trade Commission (FTC) to regulate third-party vendors

Google Analytics and HIPAA



Analytics Help

Describe your issue

Sign in

Help Center | Community | Announcements | Analytics | Contact us

Analytics for beginners | Migrate from UA to GA4 | Manage accounts, properties, and users | Manage data | Understand reports | Google Ads and attribution | Audiences and remarketing | Integrations

Data privacy and security > HIPAA and Google Analytics

It's critical that you migrate your Universal Analytics property settings to Google Analytics 4 . Starting July 1, 2023, standard UA properties will stop processing data (July 1, 2024 for UA 360 properties). Learn how to get started with Google Analytics 4.

HIPAA and Google Analytics

Google Analytics is a measurement solution that can be used to obtain business insights about traffic on your websites and apps. It is important to ensure that your implementation of Google Analytics and the data collected about visitors to your properties satisfies all applicable legal requirements.

Please remember that to protect user privacy, Google Analytics policies and terms mandate that no data be passed to Google that Google could recognize as personally identifiable information (PII), and no data you collect using Google Analytics may reveal any sensitive information about a user, or identify them. If you need to delete data from the Analytics servers for any reason, you can schedule a data-deletion request or use the User Deletion API.

What is HIPAA and to whom does it apply?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that applies to HIPAA-regulated entities. The law and its implementing regulations typically are not relevant to Google Analytics customers operating exclusively outside of the US, nor are they relevant to every customer operating within the US. Analytics customers are responsible for determining whether they are HIPAA-regulated entities and what their obligations are under HIPAA.

Can Google Analytics be used in compliance with HIPAA?

Customers must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies. Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.

For HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the HHS bulletin provides specific guidance on when data may and may not qualify as PHI. Here are some additional steps you should take to ensure your use of Google Analytics is permissible:

- Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered.
- Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages.
- Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages..
- Please work with your legal team to identify pages on your site that do not relate to the provision of health care services, so that your configuration of Google Analytics does not result in the collection of PHI.

Give feedback about this article

Was this helpful? Yes No

Need more help?

Sign in for additional support options to quickly solve your issue

Sign in

©2023 Google - Privacy Policy - Terms of Service English

Data privacy and security

- Safeguarding your data
- Privacy controls in Google Analytics
- Data sharing settings
- Manage user consent
- Consent mode on websites and mobile apps
- Google Analytics opt-out browser add-on
- [UA] IP masking in Universal Analytics
- [GA4] Policy requirements for Google Analytics Advertising Features
- [UA] Security and privacy in Universal Analytics
- We use our own products
- Data Processing Terms
- Data retention
- [GA4] Data-deletion requests
- Data deletion requests (Universal Analytics)
- ISO 27001 Certification
- Google Analytics links overview
- Account setup with additional privacy features
- Best practices to avoid sending Personally Identifiable Information (PII)
- Policy Against Fingerprints and Locally Shared Objects
- Data controls in Universal Analytics
- Data controls in Google Analytics 4
- [GA4] EU-focused data and privacy
- HIPAA and Google Analytics

Choose your own learning path

Check out google.com/analytics/learn, a new resource to help you get the most out of Google Analytics 4. The new website includes videos, articles, and guided flows, and provides links to the Google Analytics Discord, Blog, YouTube channel, and GitHub repository.

Start learning today!

Joint OCR/FTC Letter to Health Care Providers (July 2023)

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

---

[1] *See, e.g.*, Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[2] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Joint OCR/FTC Letter to Health Care Providers (July 2023)

- Sent to 130 providers nationwide
- "serious privacy and security risks" related to use of online tracking technologies "may be present on your website or mobile application" and disclosing PHI to third parties
- Cite to *The Markup* article (Dec. 2022), OCR Tracking Technology Guidance, FTC enforcement action (GoodRx, BetterHelp, Easy Healthcare Corp.)
- HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI – refers to Tracking Technology Guidance
- FTC Rule and FTC Health Breach Notification Rule apply to consumer health information and entities not covered by HIPAA
- Available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

Additional Privacy Considerations

- FTC Health Breach Notification Rule
- State Privacy Laws (e.g., Washington My Health My Data)
- **Take-aways**
  - Review what tracking technologies your system is using
  - Consider when and where within your websites and portals user information may become PHI
  - Ensure that your NPP and website Privacy Policy and Terms and Conditions are up-to-date, transparent regarding use of data, and compliant with relevant state and other federal laws

OCR Guidance on Online Tracking Technologies: Risk Stratification Based on OCR Guidance

HIGH RISK

- *Authenticated web pages*
- *Unauthenticated web pages with user login and registration forms*
- *Unauthenticated pages where the user can search for health care providers or search for available appointments*

MEDIUM RISK [though note OCR likely would put this in High Risk category]

- *Unauthenticated pages that address specific symptoms or health conditions*

LOW RISK

- *Unauthenticated pages that do not serve the functions described above*

LOWEST RISK

- *Only use tracking information for Health Care Operations purposes*
- *Obtain a HIPAA compliant authorization if sharing tracking information with third parties for marketing or advertising (regardless of web page type)*

Ad Trackers and Litigation

Class Action Litigation Re: Ad Tracking Technology in Healthcare Arena

- Consolidated litigation against Meta in ND Cal.
  - December 2022 – denial of PI
  - September 2023 – order on MTD
- Litigation against hospitals and health systems
  - Meta not named as co-defendant, or severed
  - Over 50 pending federal and state putative class actions
  - Early settlements
    - Class settlement (Mass Gen, Aurora)
    - Individual dismissals
- New target defendants

HIPAA … or not

- No Private Right of Action under HIPAA
  - 65 Fed. Reg. 82601 (Dec. 28, 2000).
  - Congressional Intent
  - Nuance of agency oversight and enforcement

Lawsuits invoke:

- Federal Statutes
  - Federal Wiretap Act (ECPA)
- State Statutes
  - California Invasion of Privacy Act (CIPA)
- State Common Law Claims
  - Invasion of Privacy/Inclusion upon Seclusion

Challenges at MTD Stage

- Consent
  - Privacy Policy - specificity
  - Notice – up front (*Javier*)
  - Limitations of judicial notice
- Sovereign Immunity
- Contract Claims
  - Based on Privacy Policy
  - Implied contract theories

Meta's Litigation Position

LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Meta Says It Can't Be Blamed For Misuse Of Pixel Software

Pixel users, not Meta, are responsible for ensuring that information they collect is not transmitted back to the Silicon Valley giant with sensitive details, it argues. And the majority of web developers do, indeed, deploy the software responsibly, according to Meta.

"Calling the Pixel 'primarily useful' for spying," it says in its Thursday filing, "is like calling a car 'primarily useful' for bank heists."

Presumption Flipped

A communication is confidential under section 632(a) if one of the parties "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan*, 27 Cal. 4th at 777. "And in California, courts have developed a presumption that Internet communications do not reasonably give rise to that expectation." *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (citing and collecting authorities); *see also Rodriguez*, 2021 WL 2026726, at *7 (explaining that plaintiffs "must plead unique, definite circumstances" to rebut California's presumption against online confidentiality). The question is whether plaintiffs have shown that

HIPAA
Health Insurance Portability & Accountability Act

Communications made in the context of a patient–medical provider relationship are readily distinguishable from online communications in general for at least two reasons. First, patient-status and medical-related communications between patients and their medical providers are protected by federal law. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information); Section I.A.2 *supra* (finding that patient status is protected health information under HIPAA). Second, unlike communications made while inquiring about items of clothing on a retail website, *Revitch*, 2019 WL 5485330, at *3, health-related communications with a medical provider are almost uniquely personal. "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up." *Norman-Bloodsaw v. Lawrence Berkeley*

Order Denying Motion for Preliminary Injunction, *In re Meta Pixel Healthcare Litig.*, (Dec. 22, 2023)

Fact Questions around Consent

Meta points out, again, that it is the third-party web developers who make their Pixel-enhanced websites available to plaintiffs and their other healthcare customers, and by doing so those healthcare entities have necessarily consented to the transmission of data to Meta.

Determination of whether actual consent was given depends on what Meta disclosed to healthcare providers, how it described and trained healthcare providers on the Pixel, and how the healthcare providers understood the Pixel worked and the information that then could or would be collected by Meta. These evidence-bound determinations are inappropriate to reach on this motion.

Meta's motion to dismiss the ECPA claim is DENIED.

Order on Meta's MTD, *In re Meta Pixel Healthcare Litigation* (N.D. Cal. Sept. 7, 2023)

Take-Aways

Presenters

Jake Bernstein
Partner
Seattle
T: +1.206.370.7608
Jake.Bernstein@klgates.com

Gina Bertolini
Partner
Research Triangle Park
T: +1.919.466.1108
gina.bertolini@klgates.com

Michael J. Stortz
Partner
San Francisco
T: +1.415.882.8011
Michael.Stortz@klgates.com

K&L GATES