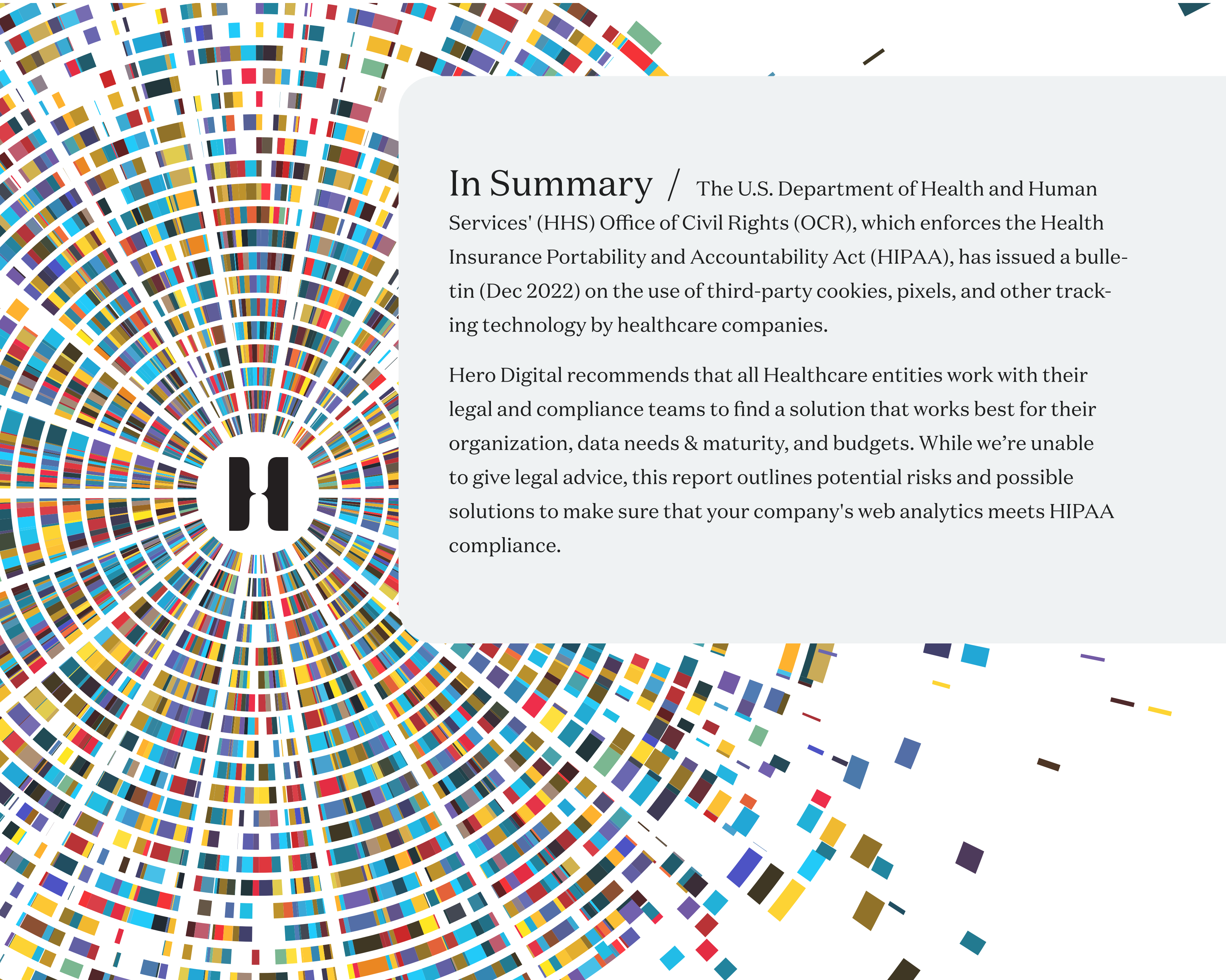
EXECUTIVE REPORT

Healthcare Tracking Compliance

Navigating Healthcare Analytics Tracking HIPAA



In Summary / The U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR), which enforces the Health Insurance Portability and Accountability Act (HIPAA), has issued a bulletin (Dec 2022) on the use of third-party cookies, pixels, and other tracking technology by healthcare companies.

Hero Digital recommends that all Healthcare entities work with their legal and compliance teams to find a solution that works best for their organization, data needs & maturity, and budgets. While we’re unable to give legal advice, this report outlines potential risks and possible solutions to make sure that your company's web analytics meets HIPAA compliance.

Hero DIGITAL

Contents

HIPPA Online Tracking: Overview

The U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR), which enforces Health Insurance Portability and Accountability Act (HIPAA), has issued a bulletin (Dec 2022) on use of third-party cookies, pixels and other tracking technology by healthcare companies.[1] The bulletin sets regulatory expectations for website and mobile app development for a wide range of companies subject to HIPAA—Covered Entities (hospitals, physician groups, health insurance plans, pharmacies, and others).

Work with your privacy and security departments to assess and mitigate risk.

- The bulletin comes as a result of a growing number of class action lawsuits concerning healthcare companies and tracking technology. Most recently lawsuits around META.
- Healthcare companies should be prepared to perform a risk-based assessment of their use of third-party tracking technology to determine Protected Health Information (PHI) is properly secured. In addition, they should work with their privacy and security departments to assess and mitigate ongoing risk as well as reassess their strategy with respect to third-party tracking.

If HIPAA covered entities and business associates use tracking technology, the Bulletin indicates that they must do the following:

- Make sure that all disclosures of PHI are permitted by the Privacy Rule and, unless an exception applies, are the minimum necessary
- Ensure that they have applicable permission prior to any disclosure of PHI and that the tracking vendor has signed a **HIPAA BAA** or that the patient signs a HIPAA compliant authorization prior to the disclosure
- Even if the vendor does not save the PHI or removes PHI before saving data, the disclosure still requires a signed BAA and permissible purpose
- Analyze the tracking technologies in the entity's HIPAA Risk Analysis and Risk Management process and ensure that transmitted PHI is properly secured

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Primary Solutions:
Google Analytics

THE OBSTACLE:

Google doesn't allow Covered Entities to enter into a business associate agreement (BAA) and because of this is in direct violation of the regulations outlined in the December 2022 bulletin. For this reason, we cannot recommend that Covered Entities stay on or migrate to Google for their website tracking.

> “Google does not intend uses of Google Analytics to create obligations under the Health Insurance Portability and Accountability Act, as amended, (“HIPAA”), and makes no representations that Google Analytics satisfies HIPAA requirements.”
> - Google Dec. 2022

HERO’S RECOMMENDATION:

We recommend potentially moving away from Google Analytics and vetting some alternative platforms that are HIPAA compliant and will enter into a BAA. Below you will find a list of platforms that fit these criteria. Freshpaint is a unique option that allows you to continue to use Google Analytics, however, leveraging their custom tracking to make your data HIPPA compliant. There would be varying additional costs associated with these options.

OTHER OPTION: REMAINING ON GOOGLE ANALYTICS - HIGHER RISK

We understand that migrating to a new analytics platform can be costly and time-consuming, so we recommend outlining an approach and timeline that works for your organization. While you're working to switch platforms, there are a few things our healthcare clients can do.

1. Turn off all Google Analytics and third-party pixels from the entire site. 100% HIPAA compliant, however, you will lose all tracking of user behaviors on your web and app properties.
2. Continue to use Google Analytics while planning your switch and make sure that Google's anonymous tracking mode is on. This change will help to ensure that no PII or PHI is being sent to Google. There is a risk associated with this as Google will not enter into a BAA and thus is out of compliance. **Please note, that staying on Google Analytics per the Dec bulletin, can leave your organization open to legal action.**

TURN ON GOOGLE ANONYMOUS TRACKING MODE.

- You can turn on users' IP anonymization by adding it to your analytics tracking code for Universal Analytics. The anonymization takes place before the user's IP address is stored in analytics. In Google Analytics 4, IP anonymization is enabled by default. GA4 is more focused on user privacy than UA, as GA4 does not rely on cookies.
- Impact: MINIMAL Google is already moving away from cookies and IP tracking.
- Additionally, you should stop Google Analytics from storing the visitorID in a cookie. We can leverage tag manager to implement this - GTM generates a new visitorID for the same visitor on every loaded page so the user can't be traced.
- Impact: HIGH This will make personalization nearly impossible and we will not be able to see user paths and conversion funnels.
- Lastly, leverage tag manager to set cookieExpires time to zero seconds. These cookies will be temporarily stored in the browser ONLY while it's open. If a user returns to the site, they will be viewed as a new user.
- Impact: HIGH This will make personalization nearly impossible and we will not be able to see user paths and conversion funnels.

HIGH-RISK AREAS

In addition to the above recommendation, Hero also advises auditing and prioritizing your analytics to ensure that the following areas are not being tracked. These have been specifically called out in documentation and involved in recent class action lawsuits.

- Tracking of customer portals/logged-in state
- Tracking of any forms or any place that a user puts in PII and/or PHI
  Appointment scheduling
- Any site search (term) tracking, inclusive of doctor search
- Search filters and pages that may identify a specific condition
  Custom dimensions
- Hyper geolocations or zip codes
  Ensure URLs are not populating any PII - users names, conditions, etc
- Adobe Connect Managed Services
- Marketo Engage
- Workfront

Primary Solutions:
Adobe Analytics

Adobe Analytics

THE OBSTACLE:

Per Adobe, out of the box Adobe Analytics is not HIPAA compliant.

HERO'S RECOMMENDATION:

Adobe has its own HIPAA-Ready services to ensure healthcare systems remain in compliance. Healthcare Shield is their full-service HIPAA solution and includes their Real-Time CDP and Customer Journey Analytics. They also offer just Customer Journey Analytics—this is their HIPAA-Ready analytics solution. These services come at additional costs. See below for more details.

Customers that license HIPAA-Ready Services to process PHI must have a BAA with Adobe that applies to those HIPAA-Ready Services. A customer may provide PHI only with a HIPAA-Ready Service, in accordance with the license agreement and BAA between Adobe and the customer. Customers are not permitted to create, receive, maintain, or transmit PHI through Adobe Products and Services that are not HIPAA-Ready Services because Adobe has not designed these services to support the customer and Adobe's HIPAA compliance.

THE CURRENT LIST OF HIPAA-READY SERVICES INCLUDE:

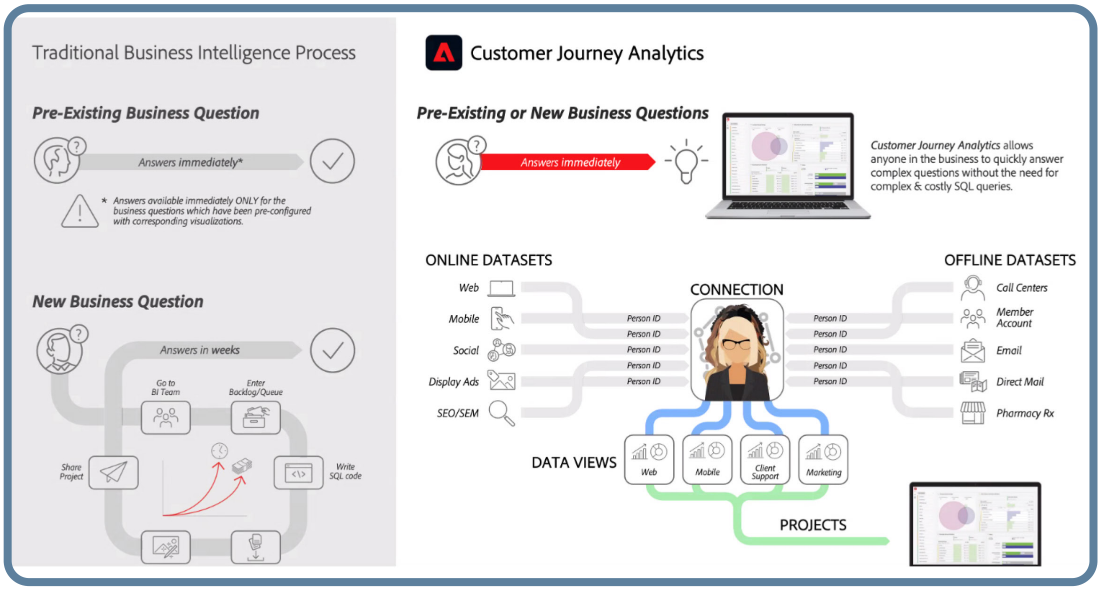
- Adobe Experience Manager (AEM) Managed Services
- Adobe Experience Manager (AEM) as a Cloud Service
- Adobe Customer Journey Analytics (CJA)
- Adobe Journey Optimizer (AJO)
- Adobe Real-Time Customer Data Platform (RTCDP) B2P (Consumer Audiences) Prime and Ultimate Editions
- Adobe Real-Time Customer Data Platform (RTCDP) B2C Prime and

ADOBE HEALTHCARE SHIELD

“Any healthcare or life sciences organization that has sensitive-data use cases and is seeking to use their data sets to better understand and serve their customers via personalized experiences will benefit from Adobe Experience Cloud for Healthcare.”

- Adobe Customer Journey analytics is included in Healthcare Shield. It also includes Adobe Real-Time CDP and Adobe Journey Optimizer
- Since this is a cloud-based solution, no on-premise CDP required.
- Adobe will enter into a BAA for this solution. This is not the case for Adobe Analytics only.

CURRENT SYSTEM FLOW



Traditional Business Intelligence Process

Pre-Existing Business Question

*Answers available immediately ONLY for the business questions which have been pre-configured with corresponding visualizations.

New Business Question

Customer Journey Analytics

Pre-Existing or New Business Questions

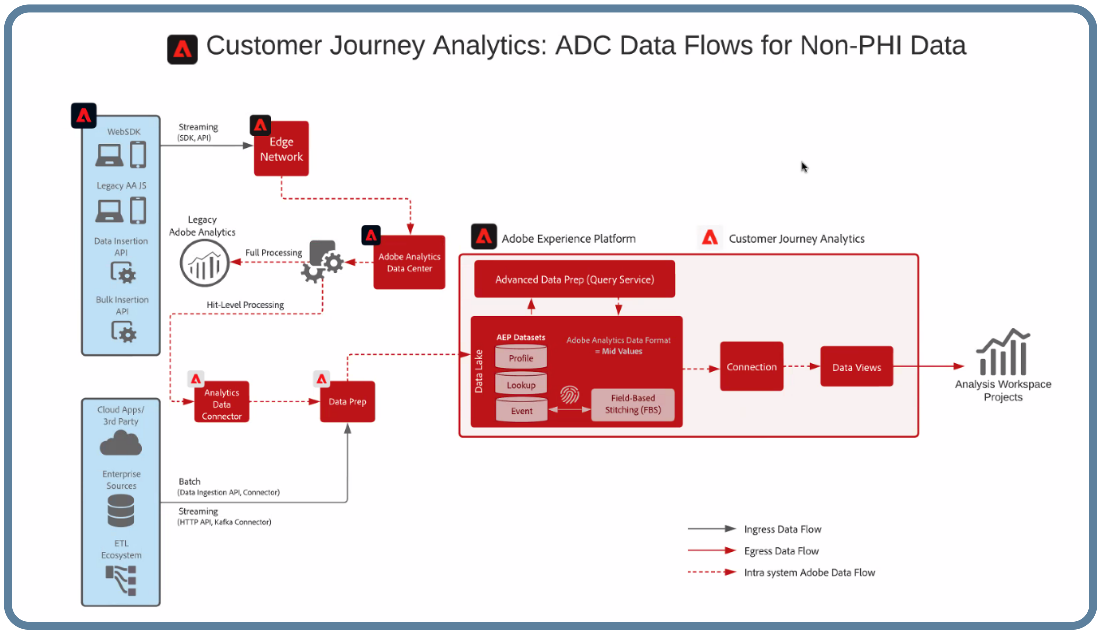
Customer Journey Analytics allows anyone in the business to quickly answer complex questions without the need for complex & costly SQL queries.

ADOBE CUSTOMER JOURNEY ANALYTICS

CJA is an Adobe HIPAA-compliant solution for analytics and an alternative to Adobe Analytics.

- CJA can be bought outside of Healthcare Shield. This would allow companies to not have to leverage Realtime CDP
- One stand-out advantage, outside of HIPAA compliance, you are able to incorporate all digital and non-digital data for true attribution.
- There would be some level of additional implementation, depending on how companies would like to use this tool and if using Realtime CDP.
- If not using HC Shield (REALTIME CDP) there is some loss of functionality. In addition, Adobe Target is not HIPAA compliant, so website testing and personalization will be difficult.

NEW SYSTEM FLOW


Customer Journey Analytics: ADC Data Flows for Non-PHI Data
WebSDK
Legacy AA JS
Data Insertion API
Bulk Insertion API
Streaming (SDK, API)
Edge Network
Legacy Adobe Analytics
Full Processing
Adobe Analytics Data Center
Hit-Level Processing
Analytics Data Connector
Data Prep
Cloud Apps/ 3rd Party
Enterprise Sources
ETL Ecosystem
Batch (Data Ingestion API, Connector)
Streaming (HTTP API, Kafka Connector)
Adobe Experience Platform
Customer Journey Analytics
Advanced Data Prep (Query Service)
Data Lake
AEP Datasets
Profile
Lookup
Event
Adobe Analytics Data Format = Mid Values
Field-Based Stitching (FBS)
Connection
Data Views
Analysis Workspace Projects
Ingress Data Flow
Egress Data Flow
Intra system Adobe Data Flow

Secondary Solutions:
Mixpanel

MixPanel - “Mixpanel’s SOC 2, ISO27001 Data Center, GDPR, and EU-U.S. Privacy Shield compliant data centers, along with our standard Business Associates Agreement (“BAA”), help our customers maintain their HIPAA compliance.”

- In accordance with HIPAA, Mixpanel is prepared and able to enter into Business Associate Agreements, or BAA.
- Mixpanel protects health information by using platform wide cryptographic controls. All data is secured in transit using TLS, and encrypted at rest in our proprietary analytics database.
- Robust reporting and data visualization
- If able to leverage their cloud hosting with a BAA, there would be no requirement to build a compliant CDP on-premise.
- Mixpanel does not allow clients to share access to other companies, therefore, the client would have to fully own this solution.

Secondary Solutions: Plausible

Plausible - “Plausible Analytics is a 100% open source web analytics tool. Our mission is to reduce corporate surveillance by making a useful and privacy-friendly website analytics tool that doesn’t come from the adtech world.”

- Open Source
- Self hosted option which would not require a BAA as Plausible would never have access to the data. **Self hosting would require the entity to build a HIPAA compliant CDP.**

Secondary Solutions: Freshpaint

Freshpaint helps healthcare providers keep their first-party customer data HIPAA-compliant by default. **You can continue to use your Google Analytics and other tools and does not require an on-premise CDP**. Safely send customer data to destinations that are not HIPAA compliant, like Google Analytics, so you can track behavior without revealing who the user is. Freshpaint's ID Masking hashes user identifiers in an irreversible way out of the box.

- Freshpaint's ID Masking hashes user identifiers out of the box so you can track customer behavior without revealing the user.
- Freshpaint's Enforced Allowlists block PHI by default, reducing compliance risks caused by human errors.
- Freshpaint is 100% HIPAA compliant with a BAA for full protection. It's purpose-built to collect, store, and manage PHI across your entire tech stack.

Secondary Solutions:

Piwik Pro

Piwik Pro - “Our product will help you act in line with data privacy regulations, such as GDPR, LGPD or TTDSG, and the CNIL’s guidelines.” “lives up to the strict requirements of Health Insurance Portability and Accountability Act (HIPAA) & EBA’s guidelines for the use of cloud service providers by financial institutions.”

- Compliant with all privacy regulations, including HIPAA, and will sign a BAA for full client protection.
- Provides three data storage options, including cloud, private cloud, and on-premise. **This gives the client the ability to implement a HIPAA compliant analytics solution without the costly need to build their own on-premise CDP.** However, Piwik Pro provides that option for interested clients.
- The analytics interface is “similar to a GA Universal Analytics”.
- Range of integration options, from data visualization to data warehousing.
- Pricing depends on hits, with potential discounts with a longer term contract.

TAKE ACTION

Take action: Hero's Approach

Hero aims to help clients navigate changing rules and regulations around data and to help your organization make informed decisions to keep their organization HIPAA compliant. We advise clients to review what we have outlined above with the legal/compliance teams to identify which solution would fit the unique needs of the business. Hero is happy to help consult and potentially help implement tracking changes or full scale implementations if switching platforms, with the guidance of the client and their legal teams.

Hero DIGITAL

555 Montgomery Street
Suite 1250
San Francisco, CA 94111

+1 (800) 760-4376

HERODIGITAL.COM