Phase2

Protect Patient Data With or Without GA4

Google Analytics' Impact in Healthcare Organizations

Google Analytics (GA) is the leader in all things data, tracking, and advertising. But what's concerning about the relationship between GA and the health and wellness industry?

As of November 2022, Google settled lawsuits regarding breaches of consumer privacy in 40 states, costing the company more than 400 million dollars. Health system class-action lawsuits regarding leaked data are underway in states such as Louisiana, California, and Massachusetts.

In the December 2022 HHS bulletin summarizing the best practices for using online tracking technologies, the Office for Civil Rights (OCR) made the following declaration:

> ***[The use of] tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions... [in combination with]... IP address... [constitutes] disclosing PHI to the tracking technology vendor.***

In plain language this information means the combination of basic information about health systems' public webpages and the user's IP address is considered Protected Health Information (PHI). While the regulation hasn't changed, this declaration raises concerns and visibility within the healthcare marketing space for one simple reason: what most used to think of as benign first-party data is now considered forbidden.

Healthcare CMOs face the critical question: How can a health organization ensure HIPAA compliance and prevent patient data, including IP addresses and location information, from being transmitted through Google Analytics? It's important to note that currently, Google does not offer a Business Associate Agreement (BAA) that covers Google Analytics.

Since Google commands the lion's share of the analytics market, they tend to be the starting context for understanding this sort of guidance. From a HIPAA standpoint, under the OCR's new guidance, it is understood that simple web tracking using GA4 on the public portions of healthcare systems' websites constitutes an unauthorized disclosure of PHI.

So What Can Be Done?

Phase2 has gathered the best options based on experience with our clients to solve these issues in real time. In considering the options, understanding the **three elements of digital data** that we are able to control is necessary. Proper handling of customer data means changing one of these three factors:

FACTOR 1

Individual Demographic Identifiers: HHS has defined 18 identifiers that are considered personally identifiable information. Chief among this list is IP Address, which many consider innocuous. Of note, the final item on that list is "Any other unique identifying number, characteristic, or code". This broad definition of what could be considered identifiable should encourage all of us to think carefully about what information is collected.

FACTOR 2

Health Information: It is widely understood that organizations should not disclose a patient's medical history. In addition, based on the HHS guidance, a public, non-authenticated Web URL that mentions a disease or condition (eg. /health-conditions/diabetes) is considered health information.

FACTOR 3

Processing Environment: That same data, transmitted to a non-covered processing environment does raise compliance concerns. But, a Covered Entity processing data and analytics inside of a Business Associate (BA) or a Covered Entity (CE) environment alleviates compliance concerns.

Option 1:
Web Analytics with a Business Associate

If the main focus is web analytics, the first option is to choose a web analytics provider who will sign a Business Associate Agreement (BAA). At this time, Google will not. By using a web analytics provider who will sign a BAA, you are changing your processing environment to alleviate those compliance concerns.

Moving to such a system allows healthcare marketers to continue to capture the detailed web analytics metrics and customer data that they are used to capturing. However, it does require training staff on a new toolset and working with vendors who are familiar with that toolset. Depending on the tool, it might not address other marketing channels such as Google Ads, Facebook, or email marketing.

Examples of web analytics providers who will sign a BAA in the marketplace include: Piwik PRO (which is modeled on Google Analytics 3), MixPanel, and Heap.

Option 2: Analytics Proxy

A second option Phase2 recommends goes by many names: analytics proxy, events brokering, or via a technique called server-side tag management.

Rather than a new software, this option is a technique of configuring the collection of web analytics. In short, web analytics data is collected and transmitted to an intermediary server that the health organization owns. The data is sanitized there to remove the IP address and any other data that might be considered sensitive. This sanitized and anonymized data is then transmitted to the web analytics software for processing.

The sanitization process removes the key pieces of demographic information. This allows one to send the sanitized health information to a non-BA processor, such as Google Analytics, Facebook, and Google Ads. This process removes the individual demographic identifiers from data being sent to web analytics systems like GA4 and can also remove the PHI from data being sent to ad tech, like Facebook.

An advantage of this approach is that it allows marketers to use their existing toolset, though in a limited manner, after revising their marketing strategy.

Implementing an analytics proxy does require deep technical knowledge to configure and maintain. It also necessitates ongoing diligence to sanitize the outgoing data. For example, when changing the data strategy (perhaps by adding new software to the martech stack), one must also update the sanitizing process. As such, it is best suited for well-staffed technology teams.

Option 3:
Customer Data Platform (CDP) with a BA Provider

A third option to consider is to use a Customer Data Platform (CDP) with a provider who will sign a BAA.

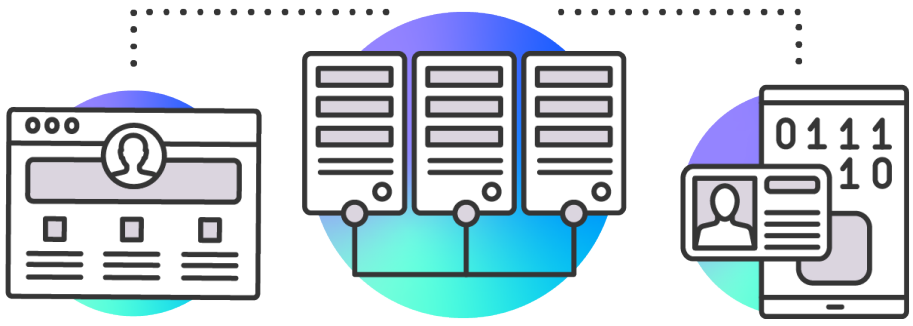
In this approach, one collects web analytics and customer data, then sends it to the CDP, which acts as an intermediary. The CDP can process and sanitize the data before sending it to downstream marketing systems.

The CDP provider manages the sanitizing process, which removes the burden from marketing teams. And, because the data is stored in a compliant environment, one is able to maintain the non-sanitized data as well, providing the best of both worlds.

A CDP is an interesting solution because it addresses needs in addition to HIPAA compliance. A CDP creates a single unified view of the customer, the "golden customer record," that is a key ingredient to first-party data in the age of the third-party cookie decline.

The CDP also helps with general compliance and the "right to be forgotten" because one can use the CDP as an inventory of the martech systems which store a customer's data.

One disadvantage of the CDP is that they are often time-consuming to deploy and require ongoing governance to maintain. Customer data is often owned by different departments across an organization—marketing, communications, fundraising—so implementing a CDP requires coordination and collaboration across the entire organization. Many CDP providers enter into Business Associate Agreements. Established end-to-end providers such as Segment, TreasureData, and Acquia CDP are well-regarded in this compliance space. Meanwhile, newer CDP infrastructure offerings such as HighTouch, FreshPaint, and Rudderstack represent composable CDP alternatives to the traditional vendors.



Product Comparison

Phase2 understands this is a situation where decisions need to be made quickly in order to comply. As a HIPAA compliant company and a Business Associate to multiple healthcare organizations, Phase2 can help your company pursue any of these options.

	Product Type	BAA Available?	Estimated Costs	Ease of Implementation	Ease of Use
GA4	Web & App Analytics	No	Varies based on dashboard usage	★★★	★★★
Piwik Pro Enterprise Cloud	Web Analytics	Yes	$	★★	★★★
MixPanel	Web & Product Analytics	Yes	$ $ $	★★	★★
FreshPaint	Analytics & Ad Platforms	Yes	$ $	★★	★★★
Acquia CDP	CDP	Yes	$ $ $	★	★★

At Phase2 we take personal information and data security seriously. We maintain comprehensive HIPAA privacy policies and procedures overseen by a designated HIPAA Compliance Officer. We take very seriously the notion of protecting confidentiality, integrity, and availability of personal data. Our people-centric approach is paramount to how we operate.

This content represents our experienced take on a topical regulatory issue affecting many healthcare organizations. Phase2 is not a legal entity, and the content in this document is not legal advice. Consult your privacy and legal team about your organization's use of Google Analytics 4.