PIWIK PRO

The guide to HIPAA compliance in analytics

The guide to HIPAA compliance in analytics

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is crucial to safeguard patients' sensitive health information, ensuring their privacy and trust in healthcare providers.

HIPAA’s main roles include:

- Mandating strict security measures to protect health records from unauthorized access and data breaches, reducing the risk of identity theft and fraud.
- Empowering patients by granting them rights over their own medical records and controlling the disclosure of their information.
- Supporting the secure exchange of health data among healthcare entities, promoting efficient and coordinated care while setting a global standard for data protection in healthcare.

Following HIPAA’s provisions means adapting to the evolving landscape of healthcare technology and data management. Non-compliance can result in significant legal penalties and reputational damage for healthcare organizations.

This whitepaper breaks down ways you can help your organization achieve HIPAA compliance in analytics, marketing and advertising, including recommended practices and tools to adopt in your technology stack.

> Disclaimer: This whitepaper is not legal advice. Piwik PRO specializes in privacy-friendly analytics software but doesn’t provide legal consultancy. Consult your lawyer for any legal clarifications or guidance on HIPAA compliance.

How to assess HIPAA compliance of marketing and analytics vendors

Your approach concerning HIPAA in marketing and analytics depends on whether you collect or process protected health information (PHI) or its electronic version (ePHI) through your site or app. Data that isn't considered PHI is outside the scope of HIPAA.

PHI and ePHI is a subset of personally identifiable information (PII) that refers explicitly to information processed by HIPAA-covered entities. Generally, when health information is combined with one of the 18 personal identifiers, the data becomes PHI.

Specific examples of PHI and ePHI include:

- Information your doctors, nurses, and other health care providers put in your medical record.
- Conversations your doctor has about your care or treatment with nurses and others.
- Information about you in your health insurer's computer system.
- Billing information about you at your clinic.

The US Department of Health and Human Services (HHS) has issued guidance on using tracking technologies that clarifies the definition of PHI. For example, it specifies that PII collected on a covered entity's website or app is considered PHI even if the individual does not have an existing relationship with the entity or the PII does not include specific treatment or billing information.

Make sure you familiarize yourself with the definition of PHI under HIPAA and strictly follow it.

If you collect PHI or ePHI, you need to follow a number of requirements to comply with HIPAA:

1a. Sign a Business Associate Agreement (BAA) with any vendor you use for marketing, analytics, advertising or any other business associate that might be exposed to PHI you handle. A BAA specifies each party's responsibilities regarding PHI and ePHI and establishes a legally binding relationship. Without a BAA, you cannot disclose PHI to that vendor without the authorization of the individuals it applies to.

> You need a BAA even if you collect data and then immediately erase or de-identify it.

1b. If you can't sign a BAA with the vendor, make sure you de-identify the data using appropriate methods. In general, de-identification involves removing all 18 identifiers from PHI so the data is impossible to trace back to one individual. Once the data is de-identified, it's no longer considered PHI, so it doesn't fall under the scope of HIPAA.

> According to the HIPAA Privacy Rule, once data is de-identified using one of the appropriate methods, you can use or disclose it without any limitation. Also, you don't have to fulfill obligations covered in other sections of this document. That said, your patient's data will be stripped of all user identifiers. You won't be able to, for example, personalize content for returning visitors, analyze patients' journeys or create detailed conversion attribution models. Additionally, because of the complicated definition of PHI, de-identification is difficult and prone to errors and HIPAA breaches.

2. Respect patient rights regarding their data, including the right to access their own medical records, request corrections, and control the disclosure of their PHI. Patients must provide written authorization for a covered entity to disclose or use their PHI.

3. Make sure you fully control and understand what data you collect, store, and transfer, who you share it with and how it's processed. Don't impermissibly disclose PHI to third parties or reuse it for other than permitted purposes.

4. Choose trusted vendors for any platforms that interact with your patients' PHI. Make sure they apply the highest security standards and HIPAA-relevant measures.

5. Implement security measures to safeguard ePHI and prevent unauthorized access, data breaches, and identity theft. You can apply the following methods:

- Encryption of ePHI.
- Access controls to ensure only authorized personnel can access ePHI.
- Monitoring employee activity, such as login attempts or password changes.
- Putting in place organizational policies and procedures for handling PHI and ePHI.
- Using backup storage with maximum recovery capability.

6. Store your data on secure, HIPAA-compliant infrastructure. You should know the exact location of your data and be able to select from different data residency options.

> In the past, many HIPAA-covered entities used on-premises hosting that didn't require signing a BAA with the vendor. However, such infrastructure is expensive and time-consuming to maintain. Currently, organizations can choose other secure hosting options that don't require as many resources, such as private cloud. Read our blog post on how to host your analytics: public cloud vs private cloud vs self-hosted to learn the differences between them.

7. Address the use of analytics and other data platforms in your risk analysis and management processes, as described in the HIPAA Security Rule.

A review of HIPAA-compliant analytics vendors

Below, we break down the HIPAA compliance of popular analytics options.

Google

In general, using Google Analytics 4 is not HIPAA-compliant because:

- Google won't sign a BAA for the use of Google Analytics.
- Google doesn't permit you to send PHI to Google Analytics. You must strip all PII/PHI from data before sending it to GA4.
- Google Tag Manager's use policy obliges you to respect Google Analytics' terms of service and not share any personally identifiable information (PII) with Google.

- Google uses all data within its systems to develop new services, improve existing offerings, and create personalized advertising experiences, which is a breach of HIPAA's Privacy Rule.

- Google stores all tracked data in databases located around the world and offers neither on-premise hosting nor bespoke data residency services. Covered entities cannot control where their patient data is stored, which is a HIPAA breach of accountability.

Client-side GTM and GA4

When using client-side GTM, the user's browser communicates directly with third parties, making it challenging to control the information being shared. Depending on how your website or app processes user information, there might be a risk of PHI being shared in HTTP requests.

This, combined with other issues concerning HIPAA and Google, rules out client-side GTM and GA4 as an option for HIPAA-covered entities.

Server-side GTM and GA4

Server-side GTM, when properly set up, helps you control what data you share with Google. User data is only sent to the server hosting the GTM container rather than being shared with multiple third-party servers. You can remove any PII within the server container before passing the data on to marketing partners. You can also host ssGTM on the HIPAA-compliant infrastructure of your choice, which doesn't necessitate signing a BAA.

You are still not permitted to send PHI to GTM or GA4, meaning de-identification will be necessary to use this setup. It's a complex and time-consuming process that requires stricter organizational measures. Any mistakes can result in sharing PHI with Google, which is a breach of HIPAA.

ssGTM, BigQuery, and data visualization tool

Because this setup doesn't use Google Analytics, it will only be affected by the difficult de-identification process. However, you can set up ssGTM with a HIPAA-compliant data collection tool and transfer events directly to BigQuery. Though this setup can be HIPAA-compliant, it remains a simple event stream that lacks the processing capabilities of analytics tools.

Adobe

Using Adobe will be HIPAA-compliant if it concerns one of Adobe's HIPAA-ready products.

Adobe Analytics with Adobe Launch

Adobe Analytics is not listed as HIPAA-ready on Adobe's site, meaning:

- Adobe won't sign a BAA with you to use AA.
- You are not permitted to create, receive, maintain, or transmit PHI through Adobe Analytics.

Adobe Customer Journey Analytics (CJA) with Adobe Launch

Adobe CJA is on the HIPAA-ready list, meaning:

- Adobe will sign a BAA with you to use CJA.
- You can safely create, receive, maintain and transmit PHI through Adobe Customer Journey Analytics.

Piwik PRO

All modules of Piwik PRO Analytics Suite help you comply with HIPAA, meaning:

- Piwik PRO will sign a BAA with you.
- You can send all types of PHI to your analytics setup and don't need to de-identify the data. Piwik PRO also helps you comply with HHS guidance on the use of tracking technologies.
- Piwik PRO offers hosting on HIPAA-compliant Microsoft Azure data centers, where you can choose the specific location of your data.
- Piwik PRO encrypts ePHI when the data is at rest and in transit.
- Piwik PRO offers advanced user-permission options that let you put PHI only in the hands of authorized personnel.
- Piwik PRO doesn't share ePHI with third parties or reuse it for other purposes.
- Piwik PRO undergoes regular privacy and security audits performed by external, independent bodies to ensure the highest level of security measures.

Common HIPAA-compliant Piwik PRO setups include:

- Piwik PRO Analytics, Tag Manager and CDP.
- Piwik PRO Analytics Suite and a data warehouse.

Read more about how Piwik PRO helps you achieve HIPAA compliance.

Using a mix of vendors

You can combine tools from different vendors, which can be HIPAA-compliant if you review the safeguards implemented by each vendor and ensure their HIPAA compliance.

Generally, your analytics setup should include the following tools:

Data collection system + data warehouse + data visualization tool

Some examples of tools that HIPAA-covered entities can consider include:

Below, we list some popular data collection systems that state they will sign a BAA, and we link to the relevant information regarding their HIPAA compliance. Aside from that, you will need to verify their specific HIPAA compliance yourself.

Data collection systems (trackers or CDPs)

- Rudderstack
- Tealium
- Freshpaint
- Segment
- Snowplow – no need for a BAA in the self-hosted version (it’s not certain whether the vendor would sign a BAA for Cloud)

Data warehouse providers

- Snowflake
- Google Cloud Platform (such as Google BigQuery)
- Microsoft Azure (such as Microsoft Azure Data Synapse)
- Amazon Web Services (such as Amazon Redshift)

Data visualization tools

- Looker Studio
- Tableau
- Power BI

> Here are examples of popular analytics setups using HIPAA-compliant vendors:
>
> - Piwik PRO (data collection, visualization, and CDP) + data warehouse (data copy for science team) + Looker Studio or Tableau (broad data visualization).
> - Adobe CJA + CDP + AEP (data collection, activation, and visualization).
> - Rudderstack (data collection, CDP) + data warehouse + data visualization tool.

Check out the table summarizing the HIPAA compliance of different analytics vendors:

	Piwik PRO	Adobe Analytics + Adobe Launch	Adobe Customer Journey Analytics + Adobe Launch	Client-side GTM + GA4	Server-side GTM + GA4	ssGTM + data warehouse + data visualization tool	Mix of vendors
HIPAA compliance	Fully HIPAA-compliant	Not HIPAA-compliant	Fully HIPAA-compliant	Not HIPAA-compliant	Not HIPAA-compliant	May be HIPAA-compliant if you take certain steps	May be HIPAA-compliant if you take certain steps
The analytics vendor will sign a BAA	✓	✗	✓	✗	✗	Google won't sign a BAA for the use of GTM. However, ssGTM may be used if combined with HIPAA-compliant tools such as BigQuery and Looker Studio or Tableau.	It depends on the tools you choose.
You can share properly de-identified PHI with the vendor	✓	✓ *	✓	✓ *	✓ *	✓	✓

* You must ensure that you don't pass any trace of PHI to these platforms. Even accidental disclosures of PHI can lead to HIPAA violations.

Compare the characteristics of the HIPAA-compliant options from the table above:

	Piwik PRO	Adobe	ssGTM + data warehouse + data visualization tool	Mix of vendors
Ease of implementation	★★★	★★☆	★☆☆	★☆☆
Interoperability	★★☆	★★☆	★★★	★★☆
Interconnectivity	★★★	★★★	★★☆	★☆☆
Diversification of vendors	✗	✗	✓	✓
Coves more use cases than “analytics+activation for healthcare”	★★☆	★★★	★★★	★★★
Raw data access	✓	✓	✓	✓
Cost	$	$$$	$$	$$$
Support	★★★	★★★	★☆☆	★★☆

Steps after you select the tool

Once you choose the right analytics vendor for your organization, there are additional requirements you need to apply to protect PHI:

- Make sure that any PHI collected on your site is visible only to authorized personnel. It’s important to educate them on the significance of maintaining the confidentiality of PHI and the potential consequences of violating HIPAA regulations.

- Consider collecting less analytics data to minimize the risk of PHI exposure. For example:

  - Don’t set PHI like email, device ID or phone as a user ID or custom dimension. Instead, use a hashed version of these identifiers.

  - Mask visitors’ IP addresses to two bytes (Level 2: 192.168.xxx.xxx). This will limit the location data to the country level and make the IP address incomplete. HIPAA considers sub-state location data and IP address as PHI.

  - Limit PHI sent in page URLs. Sometimes URLs contain data like a doctor’s visit, date of visit, name of illness or other PHI that may be visible to unauthorized personnel.

HIPAA-compliant marketing and advertising

As a HIPAA covered entity, you also need to focus on HIPAA compliance in marketing and advertising. Below, we explain a few ways to help you get started.

Marketing

Running marketing campaigns on popular advertising platforms always poses some compliance risks. Platforms like Facebook, Google, and LinkedIn Ads weren't built for HIPAA-covered entities, and none of them give you the option to sign a BAA.

How can you make your marketing HIPAA-compliant?

Consider establishing and maintaining a safe first-party data ecosystem to use the potential of PHI in a way that fully respects HIPAA.

You can use such first-party data for some compliant marketing activities, such as:

- **Onsite retargeting and personalization** help you reengage patients directly on your website or inside your app and show them special offers, discounts, or recommendations. This gives you great upselling and cross-selling opportunities.

- **Email campaigns** use another channel for promoting your offer and recommending new products to the existing customer base. In most cases, using patient data for email campaigns will require authorization. It's best if your emails focus on non-specific medical topics. For example, promote general medical campaigns, such as inviting people for free blood tests, rather than specified ones, like tests for pregnant women.

- **Improving the performance of your ad campaigns**. You can also consider integrating data from your ad platforms with a secure analytics platform, such as Piwik PRO Analytics Suite. This will allow you to evaluate the performance of your ads without sending this data back to Google or Facebook, and you can adjust your campaigns accordingly. Make sure the data doesn't leave the ecosystem of the vendor with whom you have a BAA.

Advertising

You should capitalize on advertising without retargeting and PHI, like contextual targeting. Instead of targeting individuals, create broad remarketing campaigns that don't involve PHI.

How can you make your advertising HIPAA-compliant?

Here are steps you can take for more HIPAA-compliant advertising:

- **Remove marketing pixels** from your password-protected apps and websites, such as patient portals. On top of that, consider limiting their use to your homepage, as long as you are not a clinic treating specific medical conditions. Some subpages of your website, such as blog posts about a specific disease or treatment, may still pass health information to the advertising platform.

- **Strip your data of any traces of PHI** before you push it to ad networks. Make sure to get rid of any unique identifiers and pieces of data that would allow an individual to be identified. Follow the privacy guidelines of your chosen ad platform.

- **Create remarketing campaigns based on simple and broad targeting**, for example, website visits. Here, the compliance of your ads will depend on the type of healthcare business you're in.

- **Use a safe tag management system** for better control over the information you send to the ad platforms. This way, you will control where and when the pixel is allowed to run.

If you want to learn more about how Piwik PRO can support you in being HIPAA-compliant, contact us for a custom demo:

Request a demo

About Piwik PRO

Piwik PRO makes powerful, privacy-compliant analytics software and offers high-touch support, so customers can get the most out of their data. Piwik PRO Analytics Suite provides flexible data collection and reports in addition to consent management, tag management and a customer data platform. Analytics professionals from leading organizations, such as the Government of the Netherlands, Crédit Agricole and Greiner, optimize customer and user journeys with Piwik PRO.

Contact

EMEA
+48 71 716 69 50

BENELUX
+31 858 881 458

DACH
+49 2203 989 620

NORTH AMERICA
+1 (888) 444 0049

http://piwik.pro · sales@piwik.pro