Freshpaint

The Ultimate Guide to PHI and Tracking Technology

Freshpaint

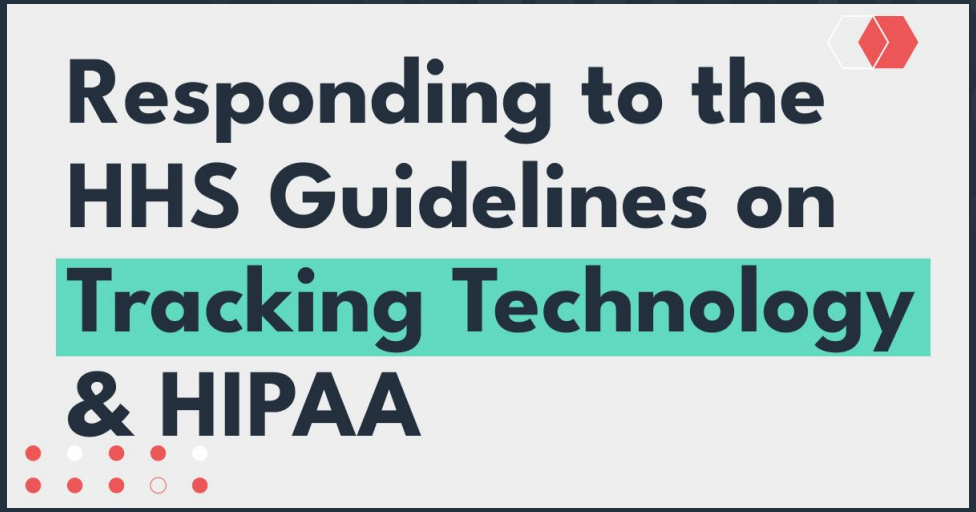
CONTENTS

Freshpaint

What Is PHI? Ending The Confusion

What did it take to get most of the healthcare world asking questions about why things like Facebook Ads and Google Analytics might put them at risk of HIPAA compliance? Try a December 2022 HIPAA update advising against Google and Facebook tracking technologies and the FTC serving notice with their $1.5M fine against GoodRx.

And two of the biggest questions marketing and IT leaders have are what exactly is PHI and what's the issue with tracking technologies. We covered why Facebook's and Google's tracking technologies aren't HIPAA-compliant in this post, but today we're going to focus on understanding PHI.



How should marketers at healthcare providers respond to new HHS guidelines? Download the ebook to learn: Common places on your website to find potential HIPAA violations, why a BAA alone isn't enough to protect you, and how to make Google Analytics HIPAA Compliant

What Constitutes PHI?

Freshpaint

The U.S. Department of Health and Human Services (HHS) says the following about the HIPAA Privacy Rule:

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- *the individual's past, present or future physical or mental health or condition,*
- *the provision of health care to the individual, or*
- *the past, present, or future payment for the provision of health care to the individual,*

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, SSN)

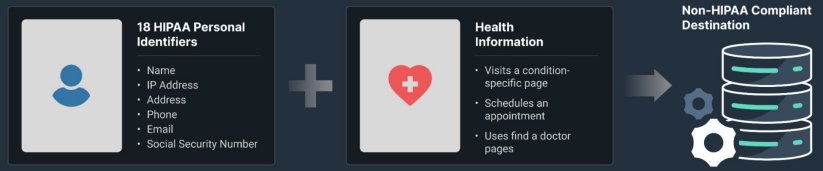
For something to be considered PHI, two things must exist:

- At least one of the 18 HIPAA identifiers has to exist.
- There is some health information.

One way for that PHI to result in a HIPAA violation:

- Sharing an identifier combined with health information with a non-compliant destination like Google Analytics, Google Ads, or Facebook Ads.

What's a HIPPA Violation?



An identifier + health information shared with a non-HIPAA compliant destination puts providers at risk.

18 HIPAA Identifiers

A HIPAA identifier is something that can reveal the identity of an individual. I know this is Ray, so I can start associating things with Ray.

HHS provides a complete list of what they consider as things that could individually identify a person. It's no surprise that something like name, email, and phone number make that list, but other not-so-obvious things can reveal an individual's identity. Let's cover a few of those.

Geographic subdivisions smaller than a state

An individual's full address would serve as an identifier, but zip codes can count too if they're small enough.

IP Address

The Meta Pixel and the tracking technologies that power Google Analytics and Google Ads sit "client-side," which means they are loaded on the physical website. Client-side loading of tracking technologies allows them to intercept personally identifiable information like a visitor's IP address.

Dates

Dates directly related to an individual, like birth date, admission date, and discharge date, are considered a way to identify an individual.

Other Identifiers Include

- Name
- Email addresses
- Phone Numbers
- Fax Numbers
- Vehicle Identification Numbers & License Plates
- Device identifiers and serial numbers
- Web Universal Resource Locators
- Social security numbers
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any unique identifying number, characteristic, or code
- Certificate/license numbers

Freshpaint

I thought Google prohibits the collection of PII?

One area where there is a lack of clarity is with Google's policy on PII. According to Google's support, "To protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII)."

The problem is that Google's definition of PII does not align with personal identifiers defined in HIPAA.

The chart to the right lists all the identifiers included in HIPAA and which ones are considered PII by Google.

Identifiers

- Name
- Email addresses
- Phone Numbers
- Addresses
- IP Address
- Fax Numbers
- Social security numbers
- Medical record numbers
- Account numbers
- Appointment and Birth Dates
- Any unique identifying number, characteristic, or code
- Vehicle Identification Numbers & License Plates
- Device identifiers and serial numbers
- Web Universal Resource Locators
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Certificate/license numbers
- Geographic Divisions Smaller than a State

Legend

Google and HHS consider this PII

HHS considers this PII but Google doesn't

Health Information

The other component required to have data considered to be PHI is health information about the individual. The HIPAA Privacy Rule calls out three categories of Health Information:

- Physical health or mental health or condition
- Provision of health care to the individual
- Payment for the provision of healthcare

Let's cover examples of each of these categories.

Health or condition

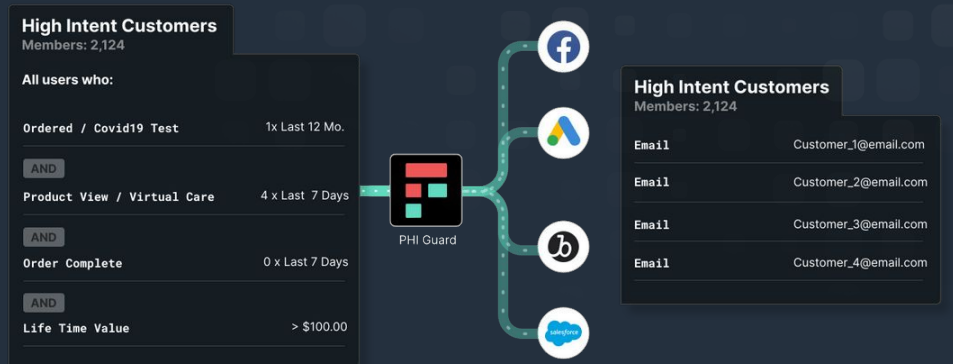
A diagnosis of type 2 diabetes or a torn medial collateral ligament would be considered health information. Tracking technologies on a hospital website could capture page visits or videos viewed that could be inferred to determine a visitor's physical health or condition.

Provision of healthcare

A scheduled doctor's appointment or medication prescription would indicate that healthcare is being provided.

Payment for healthcare

Any invoice, bill, or attempt to obtain payment for provisioned healthcare services would be considered health information.



Freshpaint guards PHI, and out of the box sends no PHI or identifiable information to your ad platforms. This makes Freshpaint safe by default and gives you control over data shared with advertisers and other platforms.

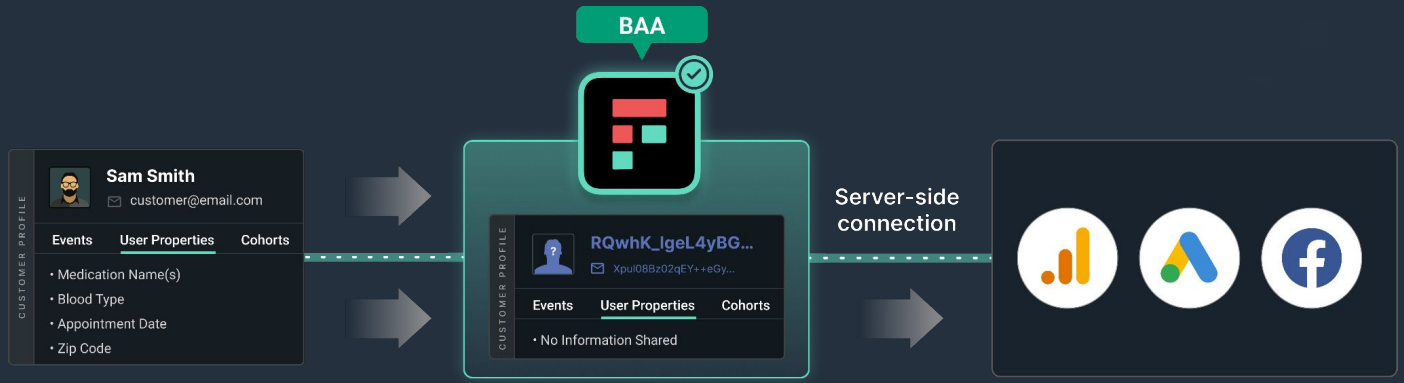
Destinations That Aren't HIPAA-Compliant

Freshpaint

This last component is where healthcare providers risk violations when running tracking technologies on their websites. Suppose you have PHI (identifier + health information about the individual) and send it to a non-compliant destination (like Google or Facebook). In that case, this information sharing has already resulted in class action lawsuits against Meta and several hospitals and the $1.5M FTC fine against GoodRx. Since Google and Meta don't and won't sign BAAs, it's impossible to use them in a HIPAA-compliant way. Or is it?

A Way to Make Your Ad Platforms HIPAA-Compliant

Digital advertising spend in healthcare is projected to be $18B in 2023. And Facebook and Google are two of the most powerful performance marketing channels. Shutting them off and redistributing the advertising spend will take years of strategic efforts for marketing teams at healthcare providers. That's where Freshpaint comes in. Freshpaint makes ad platforms and the analytics used to measure their performance HIPAA compliant while giving them the minimum data they need to drive growth effectively.



Freshpaint

How Tracking Technologies Work, And Why They Violate HIPAA

Last year, two class action lawsuits were opened against Meta and more than a dozen were filed against healthcare providers by patients throughout the US. The charge? Violating HIPAA privacy rules and sharing sensitive health information to be used in advertising and marketing.

Last month, GoodRx agreed to a $1.5 million fine for basically the same thing.

These updates to the law may feel like news for most but this has been a developing situation for many providers since January of last year. Fines and lawsuits continue to be tacked on.

If you're a healthcare provider using a Meta Pixel or tracking technologies that power Google Analytics or Google Ads, you are in exactly the same position. How these tracking technologies work is fundamentally opposed to privacy. By default, they send identifying information of individual users and health information back to Meta or Google, exactly what the HIPAA privacy rule says you can't do. In fact, since the Meta imbroglio HIPAA has updated its guidance on tracking technologies to make it explicit how you cannot use these.

So how does this technology work and how is it so incompatible with privacy and healthcare? Let's go into how companies like Meta and Google track people online. But first a quick primer on PHI so we know what we can't share about the health of users

The HIPAA Privacy rule

HIPAA's privacy rule states:

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- *the individual's past, present or future physical or mental health or condition,*
- *the provision of health care to the individual, or*
- *the past, present, or future payment for the provision of health care to the individual,*

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

That "Individually identifiable" information is important in the context of tracking technologies. There are 18 individual identifiers in the HIPAA guidelines, including "name, address, birth date, Social Security Number," but also including your IP address, device ID, or ZIP. These are all data points tracking technologies use.

Freshpaint

We did a deeper dive in a previous post about what is considered PHI in hopes of ending some of the confusion.

In December, 2022 HIPAA updated guidance to explicitly call out the risk surrounding tracking technologies. They now specifically say:

Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.

So let's see how easy it is to "use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

How tracking works

Let's say you hadn't heard about all the lawsuits and are going to add a Meta pixel to your site. The first step you'd take is to add this code:

```
<!-- 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 -->
```

So what does this do?

This isn't the tracking code as such. What this code does is set up the base code for tracking and then load the full tracking code from Meta's servers asynchronously (so your webpage won't be slowed down). The full tracking code is within https://connect.facebook.net/en_US/fbevents.js. You can see it's pretty substantial. All that code is used to track the events on each page.

Why is this called a 'pixel'? Originally it was just a 1x1 pixel that Facebook would track the loading of on each page and that would be how it would know if the page had been loaded or not. If you look carefully, you can see it still does this as a fallback through the piece of code that reads:

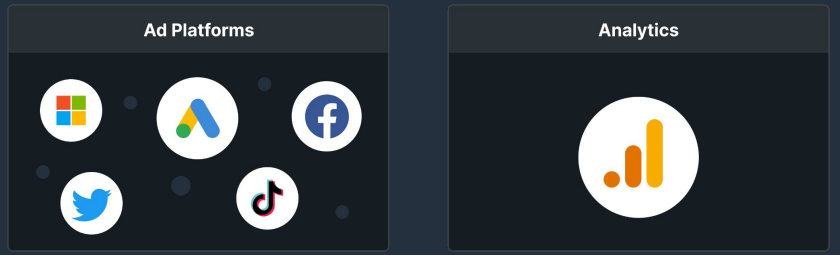
<noscript>
<img height="1" width="1" style="display:none"

src="https://www.facebook.com/tr?id={your-pixel-id-goes-here}&ev=PageView&noscript=1"/>
</noscript>

That is loading a 1x1 pixel. It is in the <noscript> tag as it's only used if you have JavaScript turned off in the browser.

So you've added that code. Sometimes there is also some configuration within the UI on Facebook to decide what you want to track. The way people usually use a Meta pixel is often to track some form of conversion on a page.

They can capture information about the person making the conversion using Advanced Matching and either a) target that person with marketing (known as retargeting) or b) feed the data from successful conversions back to Facebook so the ad platform can find similar users who are likely to convert.



HHS OCR called out tracking technology from ad platforms and Google Analytics in their advisory.

Freshpaint

To do so, Meta will track information about the user, page and form associated with any conversion (or any non-conversion). Here is what they are capturing and sending:

HTTP Headers: HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.

Pixel-specific Data: Includes Pixel ID and the Facebook Cookie.

Button Click Data: Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.

Optional Values: Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.

Form Field Names: Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.

So let's think about how this might play out on a healthcare site. You have a "schedule appointment" form on a page that's being tracked via a Meta pixel. The fields are name, email, date, and doctor. Depending on how you've set up Advanced Matching, you might be sending all this information to Facebook. If you are sending all those fields to Meta via the pixel you are definitely sending PHI and in violation of HIPAA.

A way to think about tracking technologies is this: all of the tutorials, guides, and how-tos are for regular web pages with no concern for data privacy. If you are a healthcare company and follow one of these guides, you're doing it wrong, even though Facebook is telling you you're doing it right.

Meta has two 'outs' here:

1. It says if it finds PHI in its data it strips it out and doesn't use it in any advertising
2. It uses a SHA-256 hash to 'encrypt' the data.

The problem with (1) is that it is currently being litigated in court whether this is true:

In the complaint, the patient said that Meta harvested sensitive medical information through UCSF and Dignity Health's patient portals, then sold the data to pharmaceutical and other companies which fed her targeted advertising related to her medical conditions.

This is retargeting. Likely, UCSF and Dignity have tracked the actual form fields on their site (not just the names) and passed these to Meta, who have used them to build up an advertising profile for this user, and then acted upon that information. It's exactly how adtech tracking is supposed to work, but not in healthcare.

The problem with (2) is that, though SHA-256 hashes are unbreakable, they are also deterministic, meaning that the same plain text will always produce the same encrypted text. So all you need is a long list of plain text with associated encrypted text and you can quickly look up and 'decrypt' the code. For instance, if we SHA-256 hash the word 'pregnancy' with this tool we get:

F1d6a553546aa7a9682463059f40e5a2a737b53719f0301b93d daae3fb8efaf6

Which we can decrypt with this tool:

Hash	Type	Result
f1d6a553546aa7a9682463059f40e5a2a737b53719f0301b93ddaae3fb8efaf6	sha256	pregnancy

You might think that if you don't have form data this isn't a problem. But you are still going to have a problem. First, because it is sending button data by default. This is more of a gray area, but if that button is something like "contact psychiatry," PHI can easily be inferred.

Second, is the huge problem of those "HTTP headers." This is the fundamental trap of tracking technologies–they track stuff. Their entire raison d'etre is to track a) a person on b) a page. To do that, they need some way to identify a person, so use the IP address, and a way to identify the page, so use the URL.

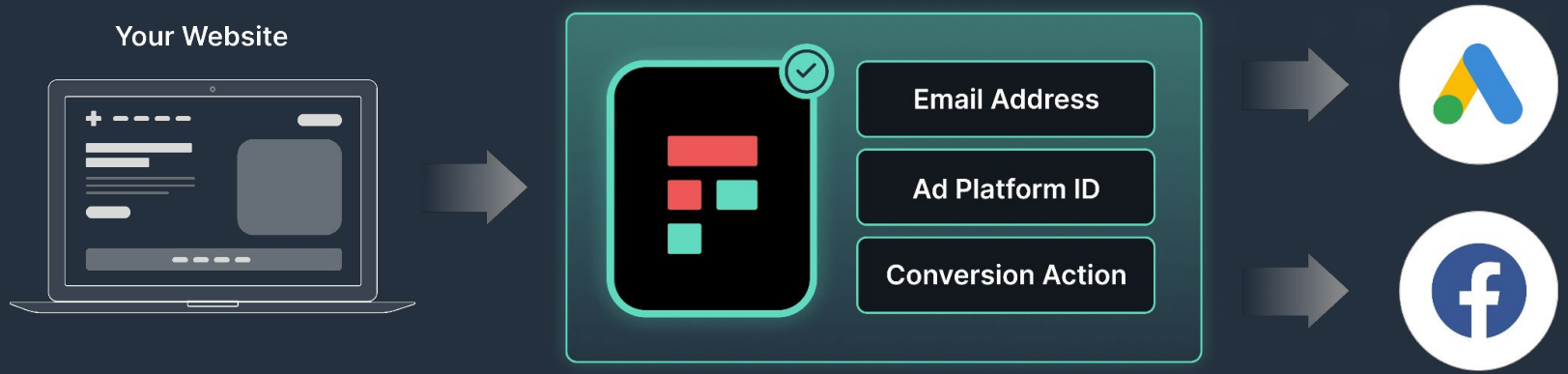
Freshpaint

The IP address is one of the HIPAA identifiers, and if the tracked page contains health information you have the recipe for what's prohibited under the HIPAA privacy rule when it comes to tracking technologies.

Here we've concentrated on Meta for two reasons:

1. They are the ones currently in court
2. They have better documented their tracking tools

But Google works pretty much the same way. It is trying to tie an individual to events on a page so that they can build up a profile of that person and serve them ads further down the line.



Freshpaint blocks health information from flowing to ad platforms, allowing your ads to be optimized around conversions while keeping you HIPAA compliant

Freshpaint

Using Freshpaint for HIPAA-Compliance

All this would be OK if Meta and Google could be trusted with PHI, but they can't. In their defense, they know they can't be trusted–that's why they won't sign a BAA.

If you have a Meta pixel, Google Analytics, or Google Ads tracking installed on a healthcare website or product, you must stop sending that data directly to these companies. But you don't have to abandon the ad platforms or the analytics you use to measure your site's performance. The simplest path forward is to replace your Facebook and Google tracking technologies with Freshpaint.

Instead of your data going from website -> unsafe tracking technologies -> Facebook/Google, it goes website -> Freshpaint -> Facebook/Google. Doing this allows you to continue using your ad platforms and analytics by taking advantage of Freshpaint's HIPAA compliant platform.

So, how does Freshpaint keep Facebook Ads, Google Ads, and Google Analytics HIPAA-compliant?

- **BAA For Full Protection**. Freshpaint signs a BAA and is purpose built to collect, store, and manage sensitive data across your tech stack.
- **Safe by Default**. Freshpaint's default state is to never send ANY data to non-compliant tools
- **Server-Side Implementation**. Unlike tracking technologies that install client-side on a provider's website, making them vulnerable to intercepting identifiers and health information, Freshpaint is only implemented server-side to give you control over your data.
- **Built-in De-Identification**. Freshpaint masks user identifiers irreversibly. No downstream analytics tool will have access to raw identifiable information about a user.
- **Forced Allowlists**. By default, no data is sent to non-compliant destinations such as Google or Facebook Ads. Instead, you choose the data and events you want to continue to send, eliminating the risk of accidentally sending PHI.

Freshpaint

Freshpaint's approach allows you to continue leveraging your ad platforms and analytics tools, but in a HIPAA-compliant way. Meta, Google, and pretty much all tracking technologies just aren't set up for industries where privacy is essential. If you are running marketing, security, or development of these types of sites, you are in serious jeopardy if you are sending data using those tracking technologies.

If you want to learn more we wrote a free guide to making your ad platforms and Google Analytics HIPAA-compliant.

two chairs

*"The killer thing about Freshpaint is the ability to control the flow of PHI to various destinations is a **super powerful unlock**."*

Scotty Abramson
Director of Growth

Freshpaint

Why You Need More Than Just A BAA To Manage PHI

If you are building health tech, the management of your users' data is a huge responsibility. They are putting their trust in you to safeguard some of their most sensitive information.

Living up to that responsibility is difficult. You have to engineer not just your product to protect this data, but anytime you have to send that data anywhere you are opening up the possibility of exposing PHI, and a chance to lose that trust.

At Freshpaint we take this responsibility seriously as well. If your users' data is flowing through our product, we help handle it correctly. Part of that is signing a BAA, or Business Associate Agreement, but there is much more to correct handling of data than legal documentation.

Here we're going to take you through a framework for thinking about compliance with the HIPAA privacy rule, and how we are doing things differently at Freshpaint.

Freshpaint

4 approaches to HIPAA compliance

Before we start, here's what the privacy rule says:

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- *the individual's past, present or future physical or mental health or condition,*
- *the provision of health care to the individual, or*
- *the past, present, or future payment for the provision of health care to the individual,*

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

So there are two parts to this:

1. the health information itself, and
2. individual identifiers.

It's the second part here that causes problems, especially with the way modern products work. Those individual identifiers are part of the dataset that teams need to improve products and marketing campaigns, understanding problems, and communicating with users. Let's say you're tracking a user interacting with a page on your site (HHS updated their guidance in December, 2022 to specifically call out tracking technologies). The tracking payload might look like this:

```
{
 "userId": "507f191e810c19729de860ea",
 "context": {
  "device": {
   "id":
"B5372DB0-C21E-11E4-8DFC-AA07A5B093
DB",
   "advertisingId":
"7A3CBEA0-BDF5-11E4-8DFC-AA07A5B093
DB",
   "adTrackingEnabled": true,
   "manufacturer": "Apple",
   "model": "iPhone7,2",
   "name": "maguro",
   "type": "ios",
   "token":
"ff15bc0c20c4aa6cd50854ff165fd265c838
e5405bfeb9571066395b8c9da449"
  },
  "ip": "8.8.8.8",
  "locale": "en-US",
  "location": {
   "city": "San Francisco",
   "country": "United States",
   "latitude": 40.2964197,
   "longitude": -76.9411617,
   "speed": 0
  },
 "network": {
   "bluetooth": false,
   "carrier": "T-Mobile US",
      "cellular": true,
   "wifi": false
  },
  "os": {
   "name": "iPhone OS",
   "version": "8.1.3"
  },
  "page": {
   "path": "/integrations/",
   "referrer": "",
   "search": "",
   "title": "Integrations",
   "url":
"<https://www.freshpaint.io/integrations>"
  },
  "groupId": "12345",
  "groupId": "12345",
  "timezone": "Europe/Amsterdam",
  "userAgent": "Mozilla/5.0 (iPhone; CPU
iPhone OS 9_1 like Mac OS X)
AppleWebKit/601.1.46 (KHTML, like Gecko)
Version/9.0 Mobile/13B143 Safari/601.1"
 },
 "timestamp": "2022-12-10T04:08:31.905Z",
"traits": {
  "name": "Ray Mina",
  "email": "ray@freshpaint.io",
  "plan": "premium",
  "logins": 5
 },
}
```

Freshpaint

There are 18 individual identifiers. 8 of them are in this single payload. The two obvious ones are name and email, but these six would also be classed as PHI:

- userId
- url
- device id
- IP
- timestamp
- city, latitude, and longitude

You can strip out some (which comes with an engineering overhead) but others, such as the URL here, are necessary to understand the journey of the user on your site. Maybe you can also strip out name and email and userId, but then you lose the ability to use those identifiers in downstream tools. If you don't send the user identifier to downstream tools those tools, like Mixpanel, are useless because you can't attribute any actions to a user so it's impossible to get a view of the buyer journey.

You're stuck between sending them and being non-compliant and not sending them and losing insight.

So how do you square this circle? You have four possible avenues:

1. Turning off analytics

2. Rolling your own

3. Using an alternative analytics tool

4. Using a CDP purpose-built for healthcare like Freshpaint

Freshpaint

1. Turning off analytics

Going lights out is undoubtedly a way to stay HIPAA compliant. If you've been building a data-driven culture, this is also the way to A) lose valuable employees that become frustrated and B) lose the ability to use data to improve visitor and member experience on your site.

Most healthcare systems have spent years building out their reporting to continue providing the best possible experience - losing that view doesn't just impact morale. It can have an impact on the bottom line.

Losing access to tech tools can directly affect the bottom line. When Tenet Healthcare experienced a cyberattack and was forced to shut off parts of its tech stack, it reported a $100 million unfavorable impact in its Q2 2022 earnings report.

Do this if

you want to make decisions based only on your gut.

Don't do this if

you think having a more complete view of the visitor journey is imperative to building a world class experience.

Freshpaint

2. Rolling your own

This is the first genuine option. You can build custom tracking and integrations for your product. The problem here is the time and cost involved. You need to build separate data pipes for HIPAA-compliant and non-compliant destinations. As Henry Lyford, Director of Engineering at Two Chairs (Director of Eng), told us that's the cost of a full-time engineer:

"To maintain customer data internally you have to have your own library for tracking events. You need to have a bunch of database tables. You'd have to make your own data to go to some visualization platform, which would be annoying. I could see this being an entire engineer's time."

If you are trying to integrate with analytics, advertising, or marketing tools, this is also the first time a 'BAA' might come into the conversation.

A BAA, or Business Associate Agreement, is what you need in place if you are going to pass PHI to a downstream vendor (your 'Business Associate' in HIPAA-speak). That might be Mixpanel for analytics, Iterable for marketing, or Facebook for advertising.

A BAA sets out the terms of how a vendor will "implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information."

Some vendors, such as Hubspot, Google, or Facebook won't sign a BAA. Some vendors will, but it is on you to understand what the BAA covers, and what it doesn't. Importantly, their appropriate safeguards and your appropriate safeguards might not be the same. It could be that they say you can send X and Y data but not Z. If you pass them Z and it leads to a violation, that's on you.

Do this if: you have a specific use case, the engineering resources to support the ongoing work required, and a good understanding of the legal requirements of BAAs.

Don't do this if: you have a small team and are iterating quickly.

Freshpaint

3. Using an alternative analytics tool

Another option is to look for a replacement for Google Analytics. There are countless on-prem solutions and an equal number of analytics tools. But this is a complex change.

If you've invested time and resources deploying Google Analytics, all of that will be lost. You're going to need to reconfigure all of your events. You'll need to rebuild all your reporting. The entire team will need to be trained. And if you have downstream workflows that rely on Google Analytics data, that will all be lost.

The switching costs here will be high, and nobody on your team wants to make a change in the first place.

Do this if: you haven't invested heavily in time and money in Google Analytics.

Don’t do this if: you are iterating on your product and want safety baked in.

Freshpaint

4. Using a tracking technology purpose-built for healthcare like Freshpaint

Google Analytics as a reporting tool isn't the problem. It's the Google tracking technology that can trip you up when it comes to staying HIPAA compliant. Freshpaint replaces Google's unsafe tracking technology with a platform that is safe by default. What we mean by this is that, by default, Freshpaint doesn't send any data to Google Analytics and masks the user identifiers:

- By default Freshpaint masks user IDs irreversibly so you don't have to do custom work to create a user ID to be shared with your CDP.
- We give customers the ability to determine which elements are safe to send to destinations. We block data to non-compliant destinations by default eliminating the risk of accidentally sending PHI and violating HIPAA
- We give customers the ability to determine which locations are HIPAA compliant (you have a signed BAA) and which aren't (you don't have a BAA) - these are your separate pipes

We'll go through the specifics of these in a moment. Of course, we sign a BAA but we also have a purpose-built product that helps reduce the security footprint, eliminates the need to replace Google Analytics, and reduces costs by eliminating BAAs downstream.

Do this if: you want to still benefit from the data you get from Google Analytics but in a HIPAA compliant way.

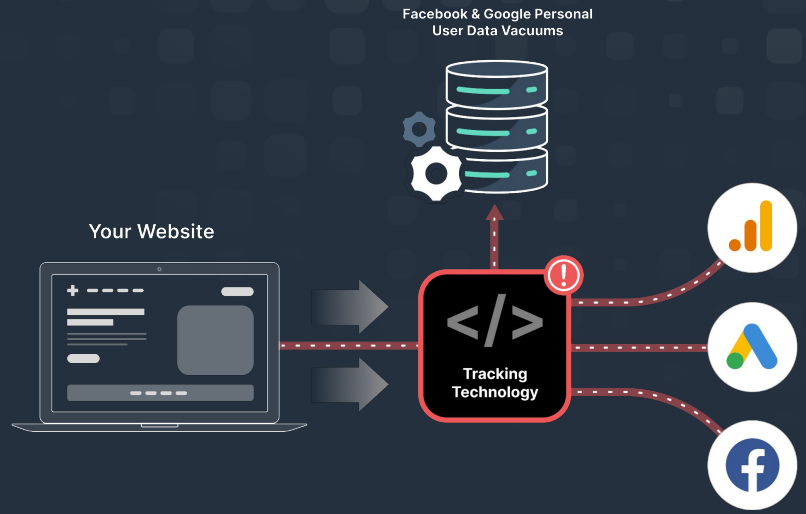
Freshpaint

How Freshpaint Keeps You HIPAA Safe

Per December's HHS guidance, a HIPAA violation occurs when collects a personal identifier and health information are sent to a destination without a BAA in place. Google, Facebook, and other ad platforms will not sign a BAA.

The problem is not with the tools themselves, but the tracking technology that is used to collect data for the platforms.

That's because those tracking technologies are like giant ad vacuums sucking up personal user data from your visitors and customers to help feed their ad businesses. The more data Google has the more powerful it is. And they're black boxes. None of us truly knows what's being ingested.



Tracking technology from Google, Facebook, and others are landing HIPAA regulated entities in hot water.

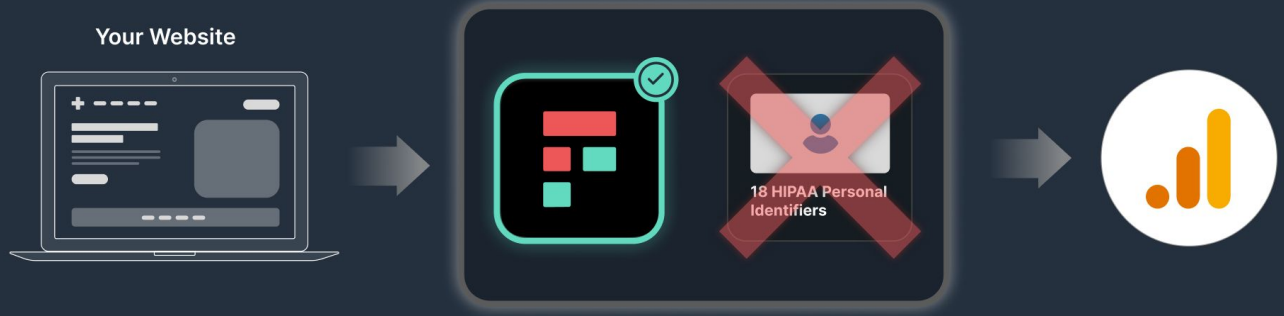
Freshpaint

Making Google Analytics HIPAA Safe

As we discussed earlier, a HIPAA violation occurs when personal identifiers and health information are shared with a non-BAA covered technology.

Freshpaint replaces non-compliant tracking technology, giving you control over what data is sent to which destinations. We sign a BAA to protect you, then use allowlists and ID hashing to keep you HIPAA safe.

For tools like Google Analytics, Freshpaint hashes identifying information. This allows you to track user journeys through your site and keep your reports and workflows in place.



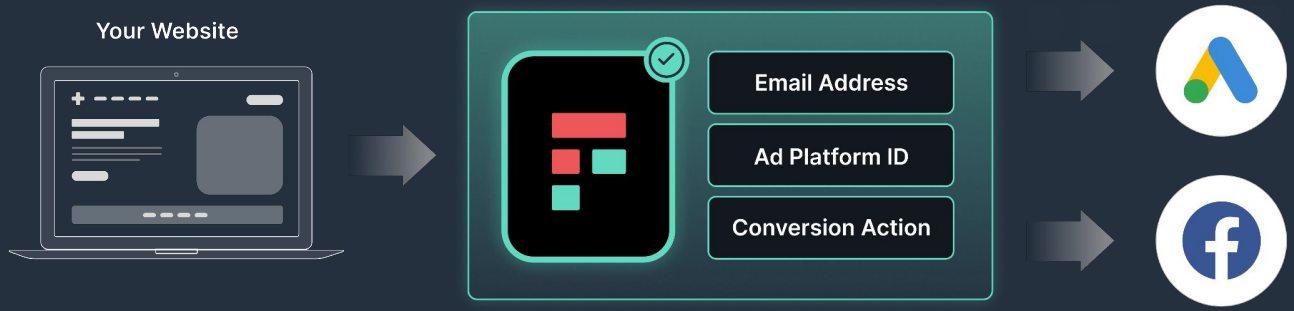
Tracking technology from Google, Facebook, and others are landing HIPAA regulated entities in hot water.

Freshpaint

HIPAA Compliant Facebook & Google Ads

Ad platforms like Google Ads and Facebook optimize ad delivery around conversions. Google and Facebook take those successful conversions and try to find more quality conversions like them using their treasure trove of data. But it's impossible to do unless Facebook and Google can identify the user.

To allow you to use the ad platforms in an effective AND safe way personal identifiers need to be shared so that the ad platform can match to the user profile they have but all health information needs to be blocked - the ad platforms don't need that information to be effective anyway. In this case Freshpaint blocks all health information while sending identifiers and that a conversion action happened. This keeps you HIPAA compliant.



Freshpaint keeps ad platforms HIPAA safe by blocking health information from flowing.

Freshpaint

How Freshpaint keeps you safe by default

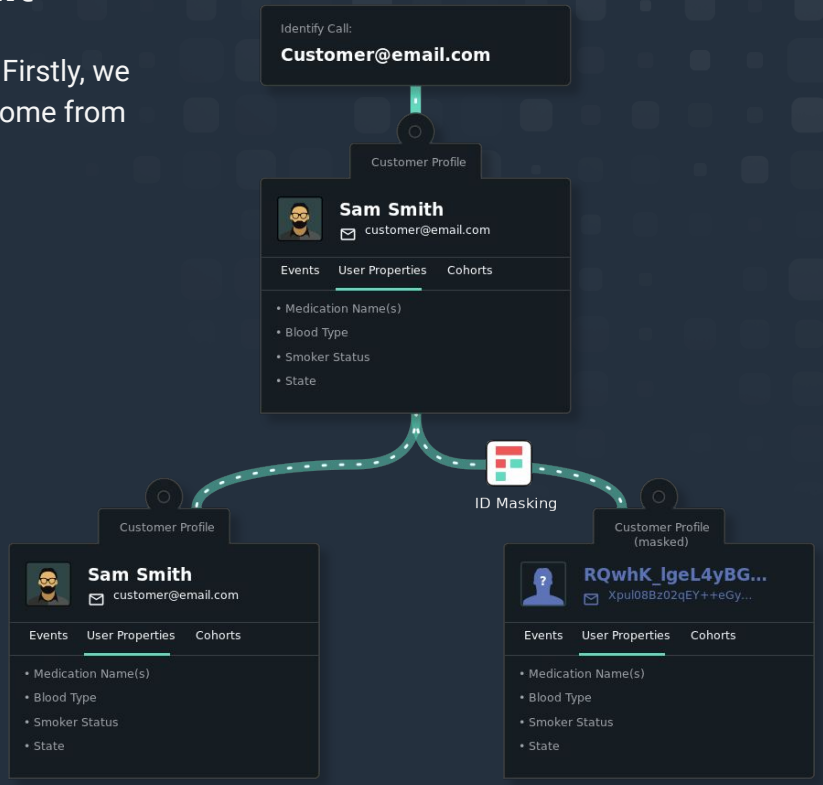
So there are three main components to how we work at Freshpaint. Firstly, we sign a BAA. But this is table stakes. Actual safety and compliance come from our ID Masking and our allowlist-first philosophy:

ID Masking

Instead of doing a bunch of custom work with a generic CDP, Freshpaint de-indentifies users automatically. This way you can still connect all the points of the user's journey in downstream tools without revealing who they are.

Our ID Masking is HIPAA compliant. We do this by:

- Using cryptographic hashing,
- with a secret key, and
- only share information server to server.



You must use a secret key because, as The US Department of Health & Human Services says:

“Code derived from a secure hash function without a secret key (e.g., “salt”) would be considered an identifying element. This is because the resulting value would be susceptible to compromise by the recipient of such data.”

Hashing without a secret key makes your data susceptible to straightforward lookup attacks and easily compromised by malicious actors.

So every identifier can have a cryptographically-hashed substitute that can still be used for product, marketing, and analytics purposes, but *can’t* be used to identify the individual.

Then all data is shared only server to server so the key is never exposed.

Enforced Allowlists

Allowlists are safer because the default is nothing is happening–no data is being sent to non-compliant destinations. Allowlists aren’t just on the integration level, they are on the event, user, and group level. This requires a little more initial setup, but for a lot more peace of mind downstream.

Manually filtering out data you don’t want to send to non-compliant destinations puts your team at risk of mistakes. Freshpaint blocks data to those non-compliant destinations by default.

First, you select the destinations that have BAAs. Then you select the events and traits that can be sent to non-HIPAA-compliant destinations. As every data point comes in, Freshpaint will screen the data, then:

- For non-compliant destinations, Freshpaint will block PHI metadata and only send masked identifiers
- For HIPAA-compliant destinations, properties can be sent as usual.

Freshpaint

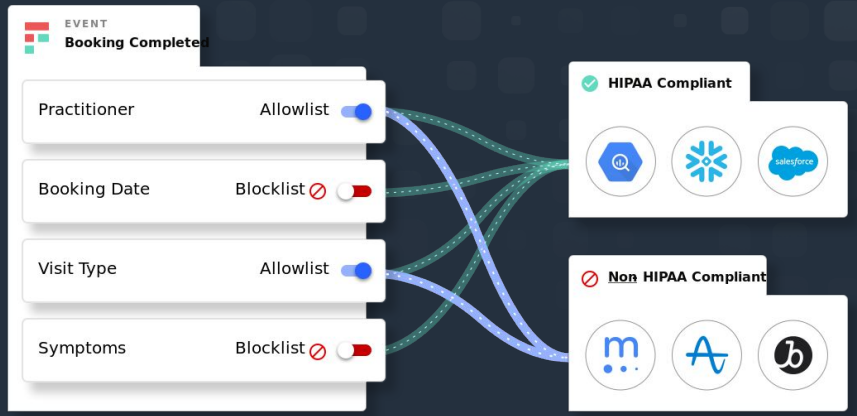
Choosing the right solution

Depending on your resources, there are several ways to stay HIPAA compliant. But if you want to stay safe by default, Freshpaint is your best choice.

When you are making this choice, you have to look beyond the BAA. Vendors will say “yes, we sign BAAs” or “We’re set up to be HIPAA-compliant” but won’t go into the details. You have to press for the details. How are they handling sending sensitive data to third-party tools? Are they hashing user identifiers by default?

All these will give you an understanding of whether the BAA/HIPAA-compliance spiel is just to cover the legalities or whether they are truly trying to safeguard your users’ data.

If you want to see how Freshpaint keeps you HIPAA-compliant and reduces your security footprint, reach out to set some time with one of our product experts.

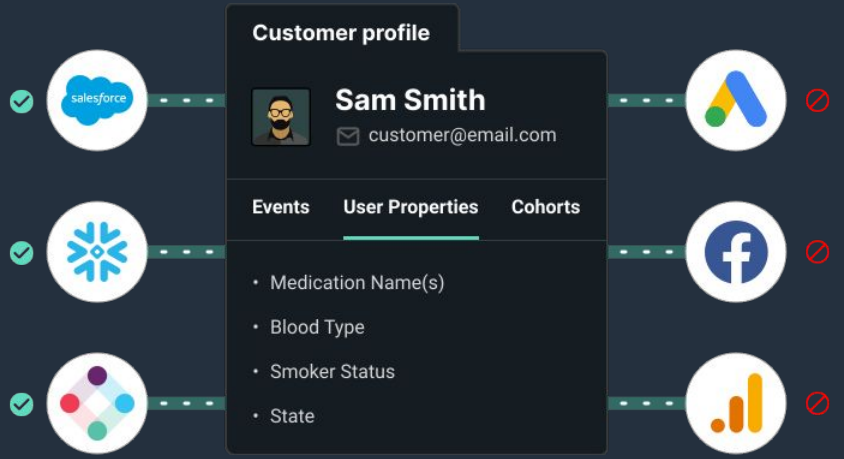


Take the Next Step with Freshpaint

December's HHS guidelines and the FTC's recent fine on GoodRX show the importance of keeping PHI secure.

Freshpaint is a customer data platform purpose built for healthcare. We help you keep first-party customer data HIPAA-compliant across the entire tech stack by default.

Click the link below to meet with one of our experts and see how we can help you keep Google Analytics and your ad platforms running while staying HIPAA safe.



Freshpaint

[Meet with one of our experts →]