Freshpaint

Marketing in a HIPAA World

A Guide for Marketers at Healthcare Providers to Navigate HHS OCR Guidance around Tracking Technologies

Balancing Privacy, Compliance, and Access to Healthcare

There's tension between providers trying to be HIPAA compliant and improving access to healthcare. HIPAA is there to rightfully protect people's privacy. To keep their personal health information out of the hands of someone who might use it in a negative way. And healthcare providers are working proactively to accomplish that.

But it also makes it more difficult for healthcare providers to accomplish their mission of improving access to healthcare for all. To do that, marketers need to meet potential patients where they are.

Like it or not, online searches and social media are how people learn about preventative medicine, new procedures, and possible cures. They aren't reading the NEJM. They're googling their pain or getting their news and information on Facebook.

HIPAA compliance makes meeting people where they are – like on Google and Facebook – much more difficult for healthcare companies than any other industry.

But not impossible. The path forward involves understanding the HIPAA guidelines and then implementing a marketing strategy that limits access to personal health information for the tools that are putting your organization at risk.

Table of Contents

What HHS Has to Say About Tracking Technologies in Latest HIPAA Guidance

When Microsoft released Internet Explorer 3.0, and President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law in August of 1996, the Internet and healthcare were very different than they are today.

The original language of HIPAA couldn't have anticipated the complexities introduced by the revolutionary changes technology has brought to healthcare. To say we've been overdue for updated guidance from the US Department of Health and Human Services (HHS) is an understatement.

In December, that guidance finally came. Hot on the heels of class action lawsuits against Facebook's parent company Meta and several large healthcare systems, HHS released HIPAA rules for companies collecting information about how users interact with their websites or apps.

What's the new HHS guidance?

The HHS specifically says:

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.

It's hard not to make a strong correlation between the high-profile Meta class action lawsuits and the timing of this update. The lawsuits accuse Facebook's Pixel (a tracking technology) of "illegal information gathering." HHS calls explicitly out "tracking technologies" in their guidance.

HHS defines "tracking technologies" as:

Generally, a tracking technology is a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app.

After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app ("website owner" or "mobile app owner" or third parties, to create insights about users' online activities. Such insights could be used in beneficial ways to help improve care or the patient experience.

According to the HHS:

The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI).

Capturing customer data to improve product experience, provide more personalized messaging, or improve ad campaigns is all certainly impacted by this new guidance. Tracking technologies are at the heart of this type of data gathering.

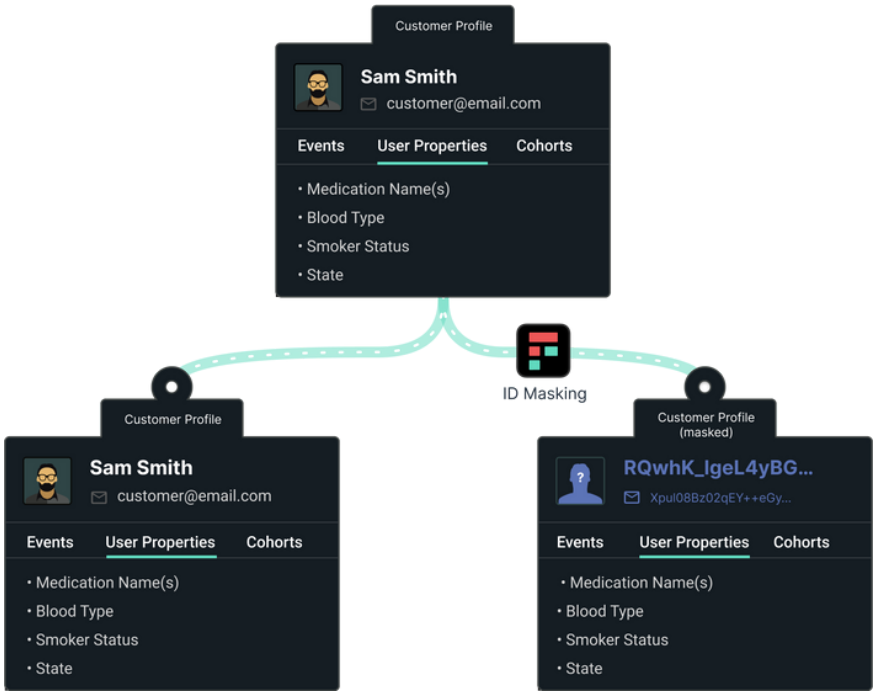
Healthcare providers of all sizes are already telling us the impact these guidelines are having. Many have completely shut off Google Analytics, leaving them in the dark about how users interact with their websites.

HHS states some of the obligations for companies handling PHI through tracking technologies:

- Disclose tracking technologies in the privacy policy or terms.
- You cannot disclose PHI to any vendor without a BAA.
- If you must disclose PHI to a non-compliant vendor, you must first have authorization from the individual.

Google and Facebook refuse to sign BAAs, so their tracking technologies are in clear violation of HIPAA.

Let's cover two scenarios to see the new guidance's specific impacts on healthcare companies...



Situation 1: I have a public website that gives information about conditions and allows users to connect with a medical professional

The Google and Facebook pixels capture a lot of information about the users visiting your websites. Things like IP address would automatically trigger a violation of HIPAA if it's linked to PHI.

Here's the language from the HHS guidance:

Individually identifiable health information (IIHI) might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.

Some specific examples where companies might get tripped up:

- If your public website contains a page where users can sign up for or login to an account (users typically enter their email or a user ID)
- If your public website contains a doctor lookup that allows users to filter by specific condition (IP address and condition now linked)
- If your public website has a page where users can book an appointment

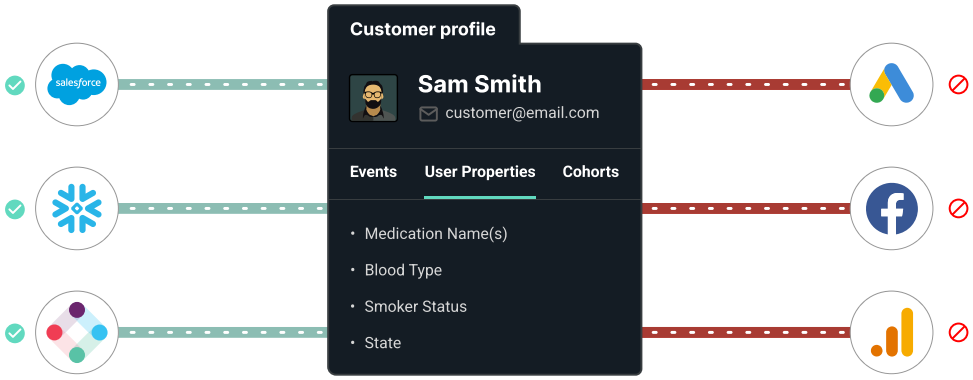
Most providers we've talked to are using tracking technologies to power Google Analytics and potentially Facebook and Google Ads. All of those tracking technologies are putting them at risk.

Situation 2: I have an app where patients book appointments, have telehealth visits and receive test results

This one is straightforward. Almost everything done in this app – from the login, appointment, conditions, and IP address is PHI and covered by HIPAA rules.

As the complexity of your tech stack scales in supporting an app like this, so do the number of tracking tools required to maintain it. Many health tech companies end up with multiple destinations for their customer data. Your tech stack might look something like this:

- Product analytics tools (many use Google Analytics at early stages and then graduate to Mixpanel, Amplitude, or similar)
- Session replay tool (CrazyEgg, HotJar)
- Chat tools (Drift, Intercom)
- Messaging tools (Iterable, Intercom)
- CDPs (Freshpaint, Segment)
- Ad platforms (Facebook, Google)



These tools are used extensively to help tech companies provide a better user experience and leverage user interactions with their application. All of these tools can inject PHI and, without the correct setup, could cause violations of HIPAA.

With HHS's new guidance, it's critical to have BAAs signed for destinations that will handle PHI. Remember that some platforms like Facebook, Google, and Hubspot won't even sign a BAA. Other tools charge extra for a signed BAA. To prevent inadvertently sharing PHI where you don't have a BAA, you'll need to invest in putting workflows in place.

What should I do now?

Here are some things you should talk about with your team:

- What tracking technologies do we have in place?
- What tools need PHI to perform their function (like emailing appointment reminders)?
- Do we have a BAA in place with all of them?
- What tools don't need PHI to perform their function?
- How do we guarantee that PHI is never shared with those tools?
- Part of HHS's guidance is to minimize the amount of PHI captured by tracking tools. What do our vendors do beyond simply signing a BAA to protect PHI?

How can Freshpaint help?

Freshpaint is purpose-built for healthcare and is HIPAA-compliant by default, whereas generic CDPs are not. What does this mean?

Bottom line is that Freshpaint can make tools like Google Analytics HIPAA compliant, so providers don't need to find a new solution.

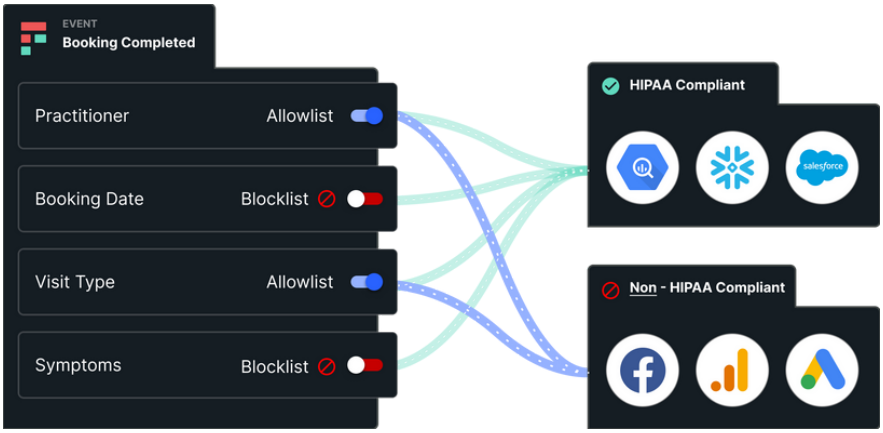
Let's dive in to understand more about how we do that.

Default hashing of user identifiers

- By default, Freshpaint irreversibly hashes user identifiers. This allows you to safely send data to destinations that are not HIPAA compliant, so you can still track that user's behavior without revealing the user's identity.
- Generic CDPs require custom engineering work to create a unique user identifier whenever you want to send data to a new destination. One customer told us this would cost a full-time engineer to manage it.

Separate HIPAA compliant from non-compliant destinations

- Your warehouse and engagement platform (like Iterable and Customer.io) are typically HIPAA-compliant. You'll need to send PHI so they can fully function.
- Send safely to non-compliant destinations (Google, Facebook, and Hubspot won't even sign BAAs). User identities will be hashed and PHI will be blocked by Freshpaint.
- Product analytics tools use data in aggregate, so you generally don't need a BAA when using Freshpaint - saving money on additional BAA-related costs.



Freshpaint blocks data from going to non-compliant destinations by default

- Freshpaint is safe by default. You must choose which data is safe to send to downstream destinations. This eliminates the risk of accidentally sending PHI and violating HIPAA.
- Generic CDPs send all the data to the destination by default. You have to select what not to send. This causes inadvertent leaks of PHI, like sensitive info in a URL, name or an IP address.

A Timeline of Events Around Tracking Technologies in Healthcare

In the Latin language of the law, there's a phrase:

Ignorantia juris non excusat

"Ignorance of the law is no excuse." The idea being that just because you don't know that it's, e.g. wrong to share medical information about patients or users doesn't mean you'll get away with it. Your ignorance is no excuse.

But for a lot of the time, HIPAA and tracking technologies have co-existed (the HIPAA Privacy Rule was initially written in 2001; Google Analytics launched in 2005; Facebook Pixel launched in 2015), ignorance does seem to have been an excuse. Healthcare companies and providers used these technologies and shared sensitive information with these companies against the HIPAA guidelines.

But 2022 was the start of an ignorance inflection point. Healthcare providers and tracking companies are now being sued for non-HIPAA compliance, journalists are investigating these compliance violations, and HHS has updated its guidance to be clear about what isn't allowed.

Even if it was once an excuse, Ignorantia can no longer exist. The suits, the stories, and the guidance are all now in front of you and clear–stop using native tracking technology if you are a healthcare provider or company.

Here's a breakdown of the nine events over the past year that have led to this inflection point.

Timeline of lawsuits, HHS guidance, and FTC fines around tracking technologies

January 2022 - Mass General settles “Cookies without consent” $18.4M

The year started with news of an $18.4 million settlement in a class action lawsuit against Mass General Brigham for “the use of cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.”

Mass General denied that any protected health information was shared, and this wasn’t a strict HIPAA-led lawsuit. Instead, the plaintiffs were suing based on a general invasion of privacy. But the large settlement showed how seriously courts were starting to take online privacy around tracking, particularly in relation to medical privacy.

June 2022 - Investigation by The Markup

A critical juncture in understanding the scope of this problem was the release in June 2022 of The Markup’s investigation into how hospitals were tracking online visitors to their websites.

The Markup looked for the Facebook Pixel on the website of the top 100 hospitals in the US. They found tracking technology on the appointment scheduling page of 33 of these sites. This means these hospitals were sending data about hospital appointments, such as dates and providers (PHI), to Facebook along with the IP address of the user (an individual identifier). This is a clear violation of the HIPAA privacy rule.

Alarmingly, they also found tracking snippets on password-protected pages of seven sites. This means they could have been sending all medical information about people visiting these pages to Meta servers.

The fallout from this investigation was huge, with a number of lawsuits against Meta (Facebook’s parent company) and these healthcare providers in the following months.

July 2022 - Class action lawsuits against Meta

Two lawsuits were immediately filed against Meta and two health systems: and the MedStar Health System in Baltimore, Maryland.

The first lawsuit also dragged in the health systems involved, the University of California San Francisco and Dignity Health. In this lawsuit, a patient claims that the Meta Pixel tool on the UCSF and Dignity Health patient portals sent her medical information to Facebook. As a result, she received ads from pharmaceutical companies specifically targeting her heart and knee issues. This is retargeting.

Retargeting is a core function of Facebook, where Facebook will serve you ads depending on how you've interacted with a previous page. It suggests UCSF and Dignity Health shared PHI about the patient's health and knee problems from their sites to Facebook in order for Facebook to know to show a related ad. Retargeting at this specificity definitely suggests a HIPAA violation.

In the second lawsuit, a patient using the MedStar Health System in Baltimore, Maryland, sued Meta saying that when she logged on, the Pixel sent her information to Facebook, including the URL of the previous page she had been on about breast health. Page URL is a PHI identifier in the HIPAA guidelines, and even though at that point the patient wasn't logged in, this can still be classed as a violation as Medstar sent both this page information about breast health and the patient's IP address to Facebook.

August 2022 - Northwestern lawsuit

One month later, a federal lawsuit was filed in Illinois against Northwestern Memorial Hospital and Meta for sharing PHI.

The plaintiff found out that his medical information had been shared through The Markup's investigation and sued for $5 million in damages because he alleged his medical information had been sold for profit. He was seeking:

- The $5 million damages
- Class-action status
- An order for Northwestern to remove any code that may jeopardize patient data.

November 2022: WakeMed, Advocate Aurora, Duke, Northwestern class action lawsuit

November brought two more class-action lawsuits against healthcare systems.

Advocate Aurora Health is a health care system concentrated in the midwest. They had been using Facebook to retarget ads based on medical tests the users had taken or the procedures they had. The PHI of up to 3 million patients had been sent to Facebook.

Advocate Aurora Health is a good example that the intent doesn't matter. Advocate said that the reason they were using tracking and targeting their patients was to improve the UX of the site and remind patients about preventative care.

WakeMed had fewer patients exposed, around 495,000. Like with many of the sites in The Markups investigation, WakeMed's appointment page had a Facebook Pixel tracking form data. This data was shared with Meta and, the lawsuit alleges, WakeMed made money from the data sharing.

December 2022 - HHS updates tracking technologies guidelines

Rounding off the year, HHS updated their guidance on using tracking technologies given all the lawsuits building. The idea here was to be more definitive about what was and wasn't allowed regarding tracking technologies and HIPAA compliance. Specifically,

"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."

"Impermissible disclosures of PHI to tracking technology vendors" is everything that had already been litigated that year and had been flagged in The Markup's investigation. The point of this guidance was to make clear two things:

1. That PHI can be anywhere on your site, not just within a patient portal. If you are tracking a public page or an appointment page, those too can include PHI.
2. Tracking within a patient portal is absolutely forbidden, no matter the intent.

February 2023 - FTC fines GoodRx $1.5M

Come the start of this year, and the news switched away from just healthcare systems to the wider problem of healthcare technology. If you are dealing with any medical information about a patient, user, or visitor, you have to follow the HIPAA guidelines.

The FTC fined GoodRx $1.5 million for "deceptively" sharing information with Facebook and other providers and "cash[ing] in on consumers' extremely sensitive and personally identifiable health information." It was serving ads to customers based on their use of GoodRx.

GoodRx also got its wrists slapped for misrepresenting its HIPAA Compliance:

"GoodRx displayed a seal at the bottom of its telehealth services homepage falsely suggesting to consumers that it complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a law that sets forth privacy and information security protections for health data."

February 2023 - Cedars-Sinai Medicine class action lawsuit

February brought another related lawsuit, this one against Cedars-Sinai Medicine for using tracking technologies on its website, where it had encouraged users to go, research, find doctors, and book appointments–all data it was then sending on to the tracking vendors, such as Facebook and Google.

The plaintiff in this case saw more health-related ads on Facebook after he had used the Cedars-Sinai website, and saw specific ads for the medical condition he disclosed on that site. A difference with this lawsuit from the other 2022 lawsuits is that Facebook isn't a defendant in this case–it's purely related to the healthcare system and its mistakes.

March 2023 - FTC fines BetterHelp $7.8M

Another fine for a healthtech company. This time BetterHelp was fined $7.8 million by the FTC for a similar breach of trust to GoodRx. Like with GoodRx, BetterHelp had told the users multiple times that all data was confidential and nothing was to be shared with a third party. But BetterHelp went ahead and retargeted ads to visitors to its site and app using sensitive information they had shared about their mental health. So people who wanted mental health help from BetterHelp saw their problems splashed across ads after they had reached out.

May 2023 - FTC fines Premom $100K and bars them from sharing data with Google

Premom violated the FTC's Health Breach Notification Rule by sharing sensitive health data to AppsFlyer and Google and failing to notify users. This one is a little bit different because it's not a HIPAA violation, but it is still a health information violation, which is controlled by the FTC.The FTC's settlement with Premom requires the company to stop sharing personal health data with third parties, obtain consent before sharing any health data for any other purpose, and pay a fine of $100,000.

July 2023 - FTC and HHS issue a joint warning about the security risks from web tracking tools

The FTC and the HHS sent a letter to 130 healthcare organizations alerting them that they might be at risk of violating HIPAA for using common web trackers like Meta's advertising pixel and Google's analytics platform. The big takeaway is that this letter isn't just a warning, it's more of an ultimatum. The letter essentially said to these 130 healthcare orgs, "Stop sharing PHI with third-party platforms or face serious consequences."

What will come next?

There can be no excuse now. If you are still using native tracking technology on your healthcare site, you are probably violating HIPAA. Stop now. If you are doing so and lying about it in your privacy policies, you are going to get fined millions of dollars. More stories like this will come out as a) the clean-up from people not understanding the ramifications continues, and b) people continue to make the same mistakes.

Don't let that be you.

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 now we'll focus on understanding PHI.

What Constitutes PHI?

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:

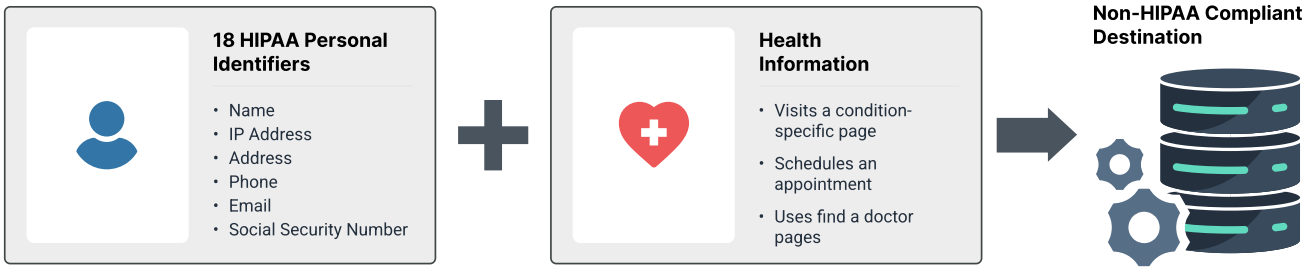
- *the individual's past, present or future physical or mental health or condition*
- *the provision of health care to the individual*
- *the past, present, or future payment for the provision of health care to the individual*
- *anything that identifies the individual or for which there is a reasonable 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).*

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

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

One way for that PHI to result in a HIPAA violation is by sharing an identifier combined with health information with a non-compliant destination like Google Analytics, Google Ads, or Facebook Ads.

What's a HIPAA Violation?



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

Let's break this down further by discussing each of the three components.

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 so would ZIP codes on their own if:

- The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people.

AND

- The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000

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.

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 below lists all the identifiers included in HIPAA and which ones are considered PII by Google.

- **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**
- **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 look at some examples of each of these categories.

Health or condition

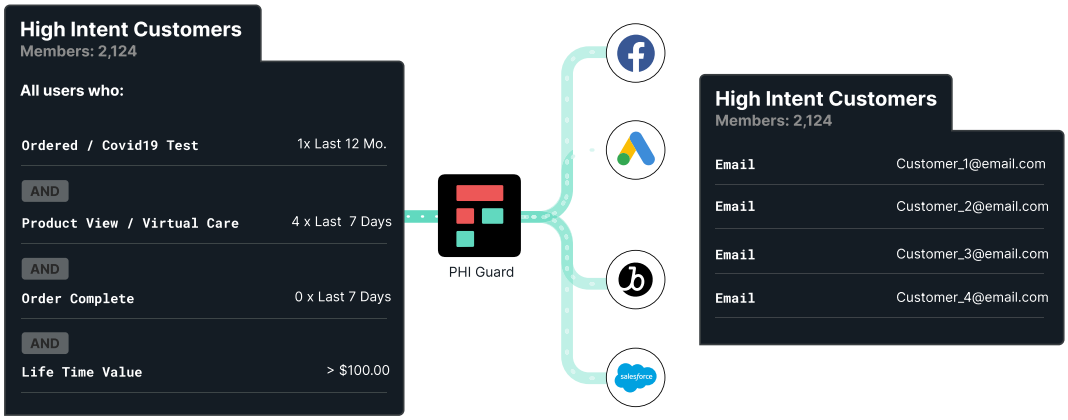
A diagnosis of type 2 diabetes or a torn medial collateral ligament would be considered health information. Tracking technologies on a hospital website could capture page visits or videos viewed that could be inferred to determine a visitor's physical health or condition.

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

This last component is where healthcare providers risk violations when running tracking technologies on their websites.

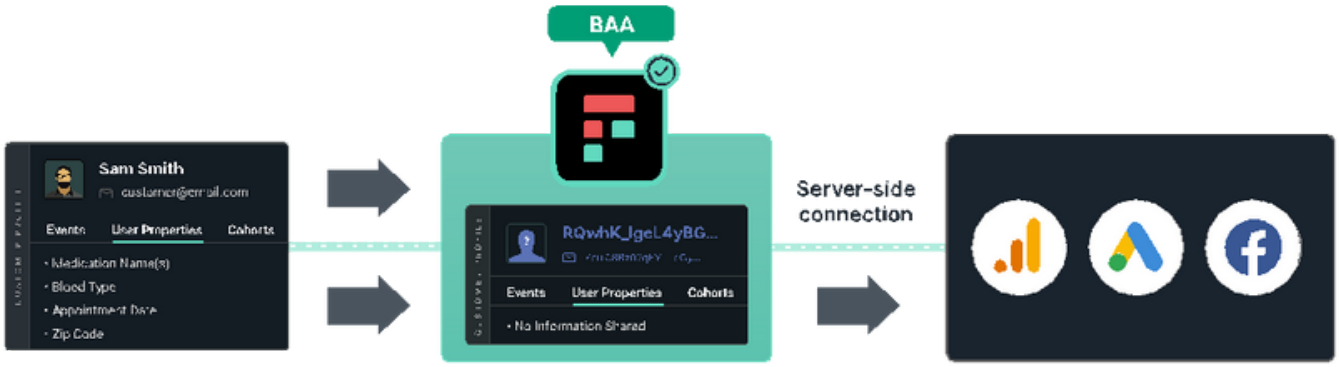
Suppose you have PHI (identifier + health information about the individual) and send it to a non-compliant destination (like Google or Facebook). In that case, this information sharing has already resulted in class action lawsuits against Meta and several hospitals as well as the $1.5M FTC fine against 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.



BOOK A DEMO

How Tracking Technologies Work, And Why They Violate HIPAA

Last year, as we mentioned earlier, 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. Additionally, GoodRx agreed to a $1.5 million fine for basically the same thing.

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 another quick primer on PHI so we know what we can't share about the health of users.

The HIPAA Privacy rule

Remember what the 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*
- *anything 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).*

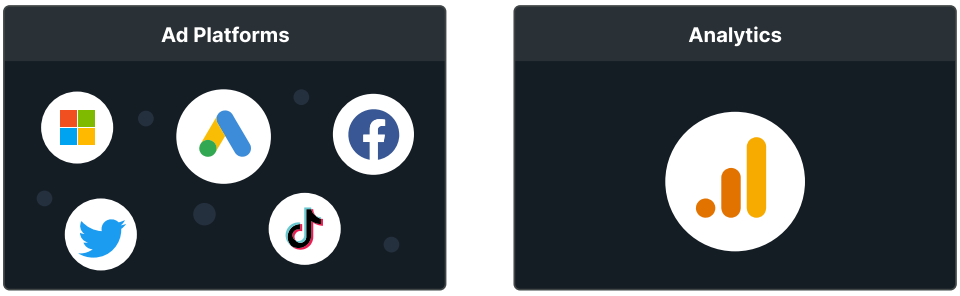
That "Individually identifiable" information is important in the context of tracking technologies. There are 18 individual identifiers in the HIPAA guidelines, including "name, address, birth date, Social Security Number," but also including your IP address, device ID, or ZIP.

These are all data points tracking technologies use.

The updated HIPAA guidance at the end of 2022 explicitly called out the risk surrounding tracking technologies, and now they 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."*



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

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.

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 an online tool we get:

F1d6a553546aa7a9682463059f40e5a2a737b53719f0301b93ddaae3fb8efaf6

Which we can decrypt with another 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.

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.

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.

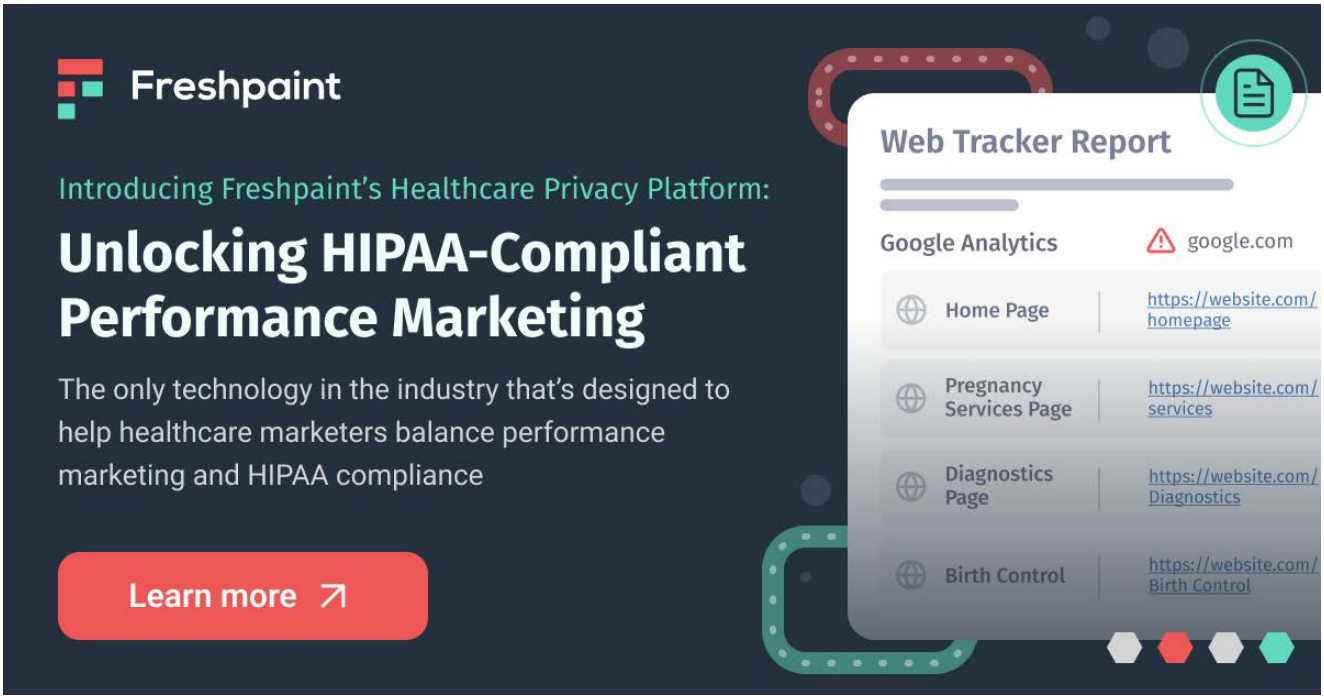
Instead of your data going from website -> unsafe tracking technologies -> Facebook/Google, it goes website -> Freshpaint -> Facebook/Google. Doing this allows you to continue using your ad platforms and analytics by taking advantage of Freshpaint's HIPAA compliant platform.

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'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, secu-rity, or development of these types of sites, you are in serious jeopardy if you are sending data using those tracking technologies.



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.

4 approaches to HIPAA compliance

Before we start, it's important to remember that the privacy rule protects all "individually identifiable health information". We've covered this several times, but the main message is that there are two parts to this:

1. The health information itself
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.

So 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-AA07A5B093DB”,
 “advertisingId”: “7A3CBEA0-BDF5-11E4-8DFC-AA07A5B093DB”,
 “adTrackingEnabled”: true,
 “manufacturer”: “Apple”,
 “model”: “iPhone7,2”,
 “name”: “maguro”,
 “type”: “ios”,
 “token”:
“ff15bc0c20c4aa6cd50854ff165fd265c838e5405bfeb9571066395b8c9da449”z },
 “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”,
“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
},
}

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

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.

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, theirappropriate 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.

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're happy with the data you get from Google Analytics and really didn't anticipate making a change.

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 send data safely to a destination like Google Analytics where a BAA doesn't exist
- 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.

Don’t Remove It! Make Google Analytics HIPAA Compliant Instead

One of the last things any web developer does as they are about to push a site live is add this code:

```
<!-- Google tag (gtag.js) -->
<script async src=”<https://www.googletagmanager.com/gtag/js?id=G-ABCDEFGH1J>”></
script>
<script>
 window.dataLayer = window.dataLayer || [];
 function gtag(){dataLayer.push(arguments);}
 gtag(‘js’, new Date());

 gtag(‘config’, ‘G-ABCDEFGH1J’);
</script>
```

Then they can sit back, relax, and know that, whatever else happens, they can track page views and sessions on their site through Google Analytics. Website Managers, Marketers, the C-suite—they’ll all be able to get their metrics buzz. Job done.

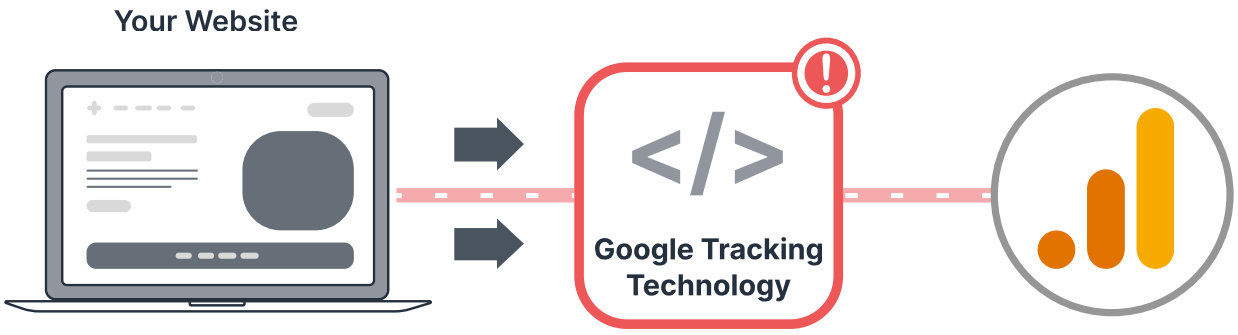
If that developer happens to be working for a healthcare provider of any kind—health tech, insurance, hospital system, any organization that deals with PHI—then they’ve just exposed their company to a huge liability.

Google’s Tracking Technology is not HIPAA-compliant

Another reminder that the HHS' guidance on online tracking makes clear that, in its basic configuration, you cannot have Google Analytics anywhere on your site that could expose both PHI and individual identifiers.

- You might think it’s OK to have this tracking pre-sign-in. It’s not.
- You might think it’s OK to have this tracking as it aggregates data. It’s not.
- You might think it’s OK to have this tracking if you have a banner telling the user they can opt-out of tracking or cookies. It’s not.

The tracking technology behind Google Analytics is not HIPAA-compliant. You cannot use GA tracking on any page on your site that might have access to PHI and individual identifiers. Here we’re focusing on Google Analytics, but it’s true for other tracking tools that don’t sign a BAA, such as Meta’s Pixel tracking, as many a class action lawsuit show.



Their reasoning for this is clear.

Say you're a pregnant woman looking for an OBGYN in the area. You google 'obgyn near me' and click on the first link, a local healthcare system's pregnancy services page. The GA tracking snippet will collect that page URL along with your IP address. This is protected health information—anyone with this data could surmise that an individual woman is pregnant.

Google Analytics does aggregate this data for you. You won't see the woman's IP address in your dashboard. But Google still has the data. And it will still tell you the general location of the viewers of that specific page, which is granular enough to fall foul of the HIPAA privacy rule.

The same could be true of a sign-in page or a scheduling page. Medical information about individuals can be inferred from the data tracked on these pages, so HIPAA rules apply if Google has access to any of these eighteen individual identifiers.

You might get away with Google tracking technology on a home page, a general services page, or an office location page. But the point of GA is it is site-wide. So if you are building or running a healthcare site, the tracking technology behind Google Analytics is putting you at a compliance risk.

This updated guidance is becoming a massive problem for healthcare providers dealing with PHI. As one team told us:

> ***"It's chaos. It's taken us seven years to create a culture of data, and it's completely up in flames."***

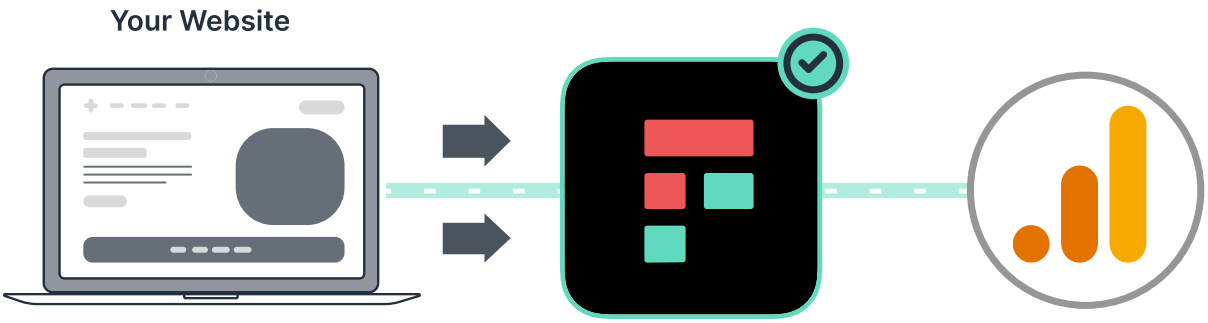
Because the data doesn't stop at GA. Google Analytics is usually just the collection point for the data that is then passed into a warehouse, a BI tool, or custom analysis. If you can't continue to use Google Analytics, an entire tool stack can go "up in flames."

Using Freshpaint to make Google Analytics HIPAA compliant

You can continue to use Google Analytics with a simple twist—you need to stop using

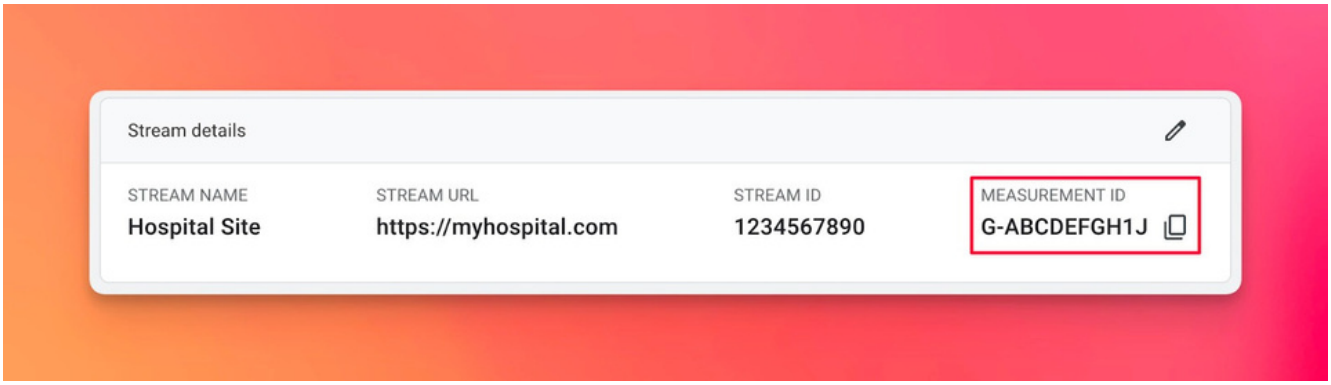
Google's tracking technology and trade it for a platform that is HIPAA compliant. We've outlined four approaches to this process in our post on BAAs and anonymizing data, including a DIY version. But if you want no interruption to your GA data, the easiest way is going to be to use Freshpaint's ID Masking and Allowlist setup:

- **ID Masking.** Freshpaint masks user identifiers irreversibly. No downstream tracking tool will have access to raw identifiable information about a user.
- **Allowlists.** By default, no data is sent to non-compliant destinations such as Google Analytics. Instead, you choose the data and events you want to continue to send to Google Analytics, eliminating the risk of accidentally sending PHI

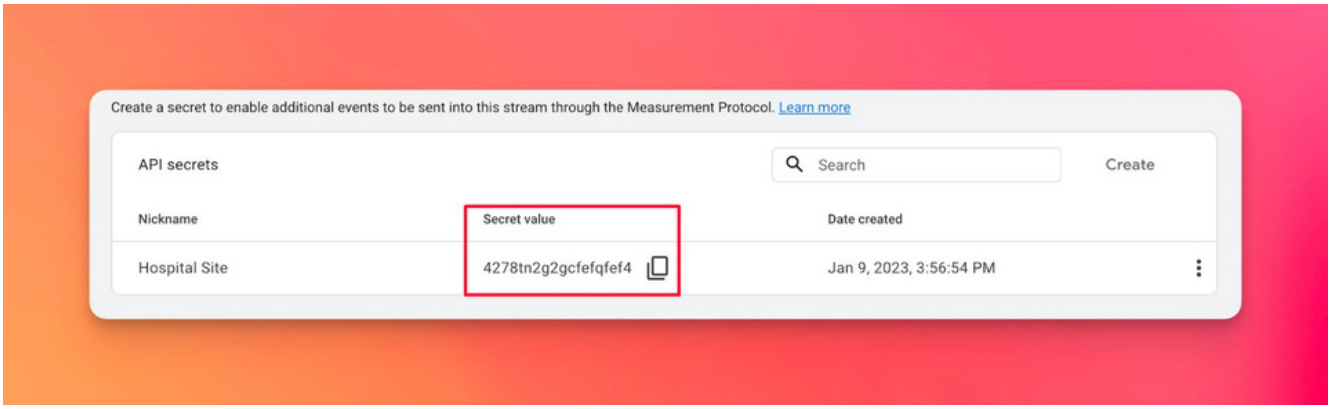


Sending data to Google Analytics through Freshpaint is easy to set up. You'll need HIPAA mode enabled, and to set up your allowlist, then you just need two pieces of information.

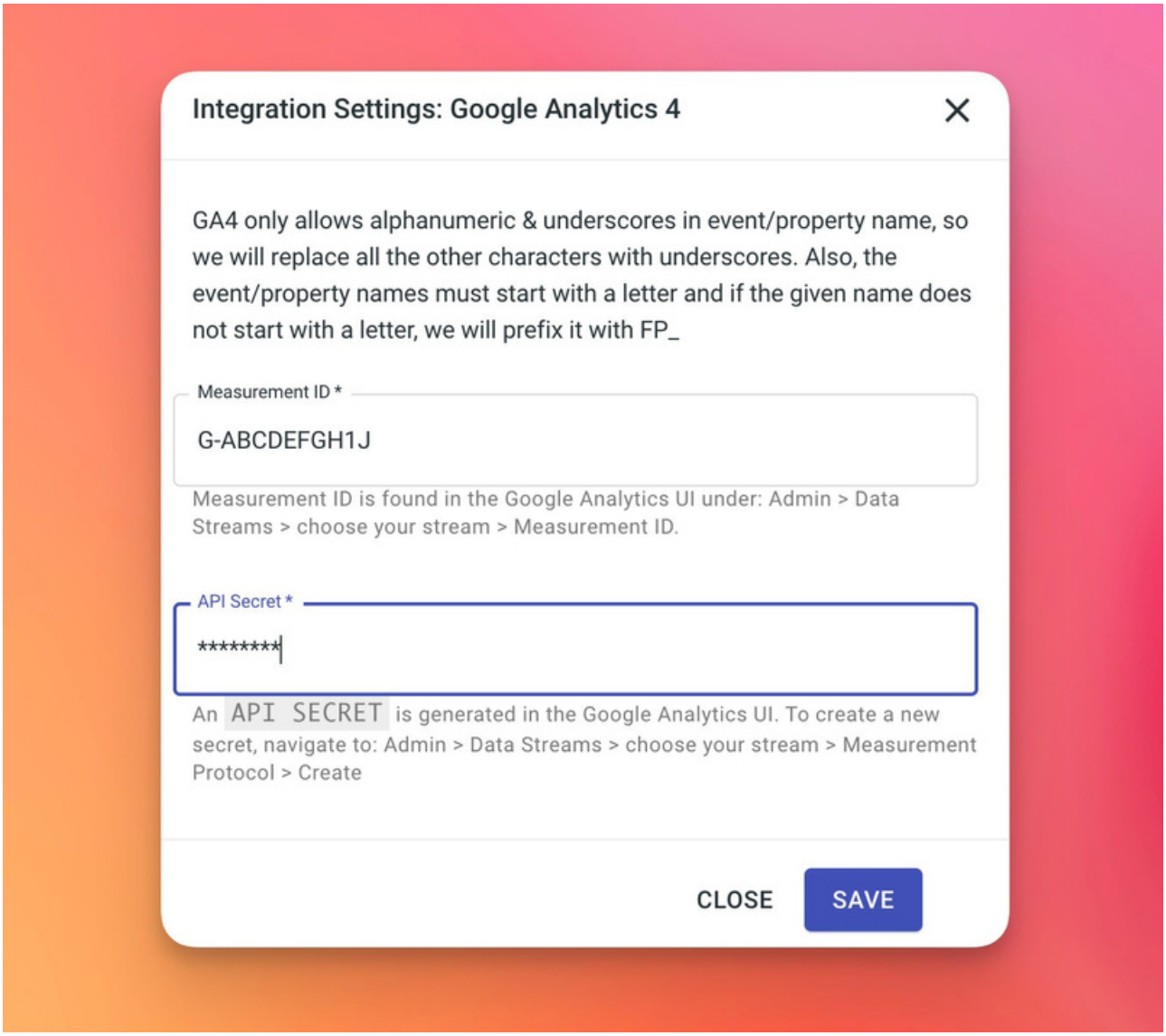
First, your measurement ID. You can get this by going to Admin > Data Streams > choose your stream > Measurement ID:



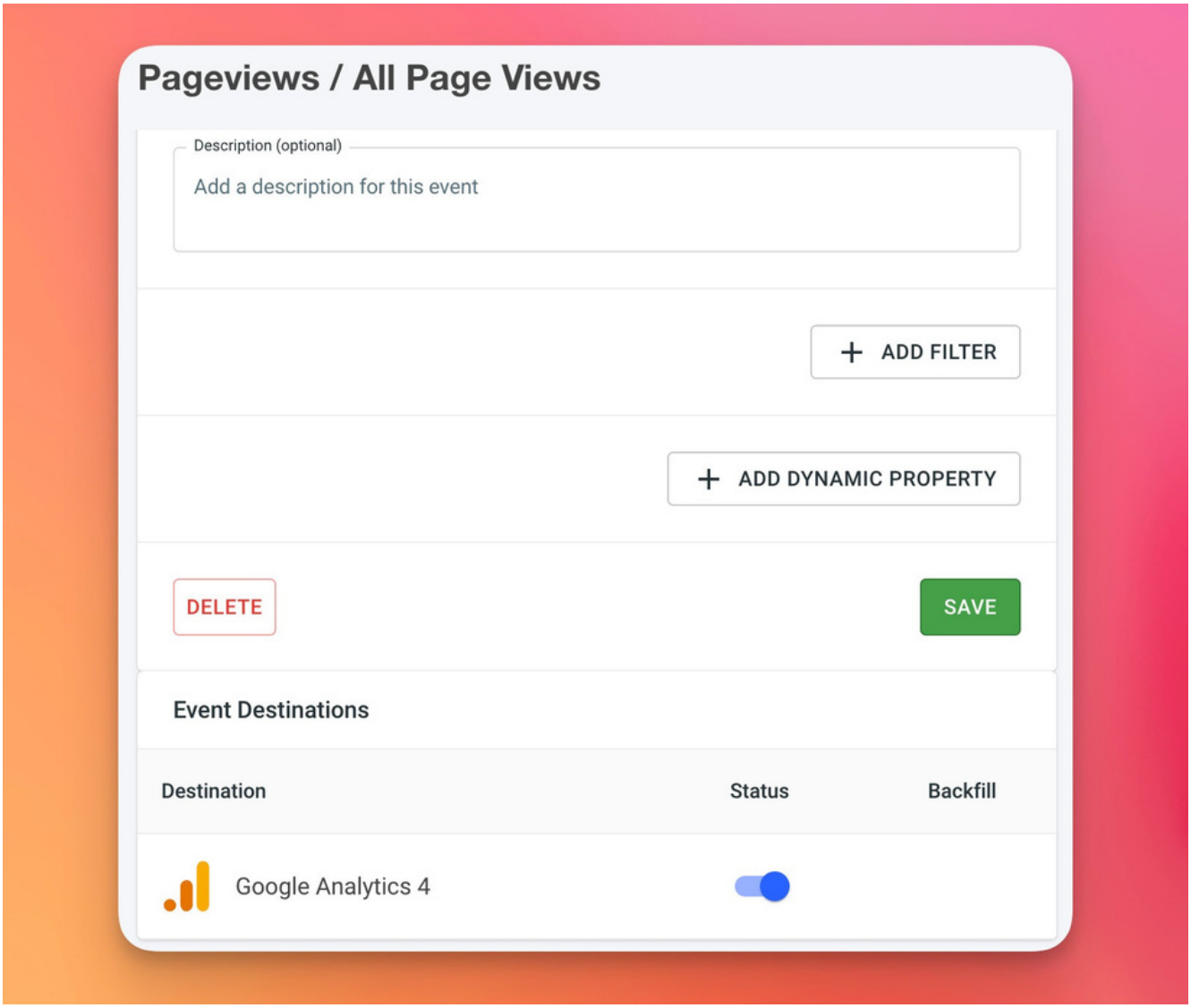
You'll also need your API secret. You can get this by going to Admin > Data Streams > choose your stream > Measurement Protocol > Create:



You can then add this information within the Google Analytics Configuration:



Then go through each of the events you want to send to Google Analytics and toggle them on:



That's it. Your data will then continue to go to the same GA property as before. As you can set this up in minutes, you won't lose data.

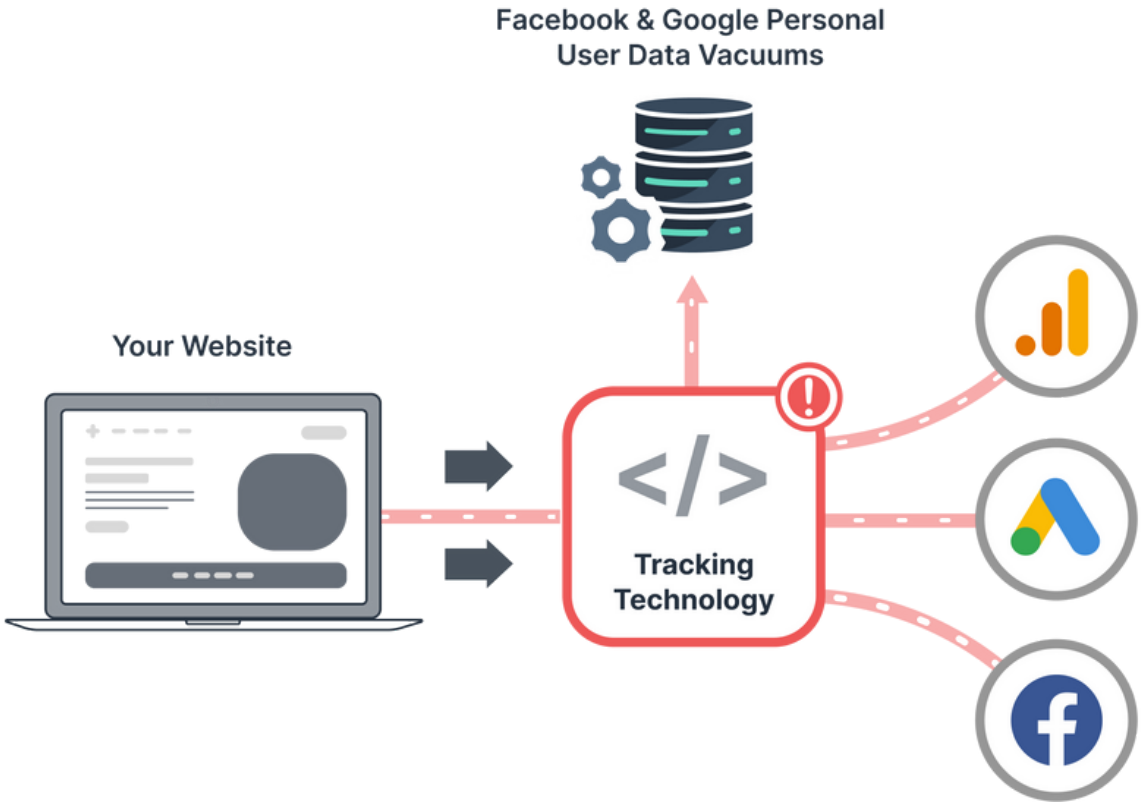
Treating your users with care

Google Analytics is a powerful tool to help give you a better view of your visitor and member experience across your site. Unfortunately, Google's tracking technology that feeds the data into GA is putting you at risk of HIPAA compliance. The answer isn't to stop using Google Analytics. The answer is to stop using Google's unsafe tracking technology. Freshpaint is the safe by default replacement so you can continue using Google Analytics and avoid losing all the work you've put into it.

How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking

Facebook Ads is another platform we've mentioned that's presenting a huge challenge for healthcare providers.

Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers. Let's remember that healthcare providers that have been using Facebook tracking are being sued by patients and have been hit with growing fines.



Meta's Pixel is like a personal user data vacuum.

If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now. We're past the inflection point for this issue now–there is enough evidence and support out there that if you continue to use Facebook's standard setup, you stand the chance of getting sued by users/patients and fined by the government.

But this doesn't mean wrecking your entire growth program. Suppose you want to continue to have ad click attribution or use a conversion-optimized bidding strategy in Facebook. In that case, you need better control over what you send to Facebook to stay HIPAA-compliant.

Let's look at how this problem arises, a few example scenarios that can get you into trouble, and how you can better control your data for HIPAA compliance and better conversion track- ing.

The Meta problem

One of Facebook's strongest value propositions is its ability to create campaigns that help advertisers maximize conversions. Advertisers can leverage Facebook's algorithm to optimize towards driving more clicks that are more likely to convert. Facebook is good at doing this, so good in fact that it helps drive a $100B annual ad business.

Let's think about how this would play out in a healthcare context. To maximize conversions, you send a successful action (say a new member sign-up) back to Facebook. Based on those new member sign-ups, Facebook will use its treasure trove of data to find more users to click on the ad that are more likely to convert.

But some fundamental things make this a no-go for healthcare providers concerned with HIPAA compliance:

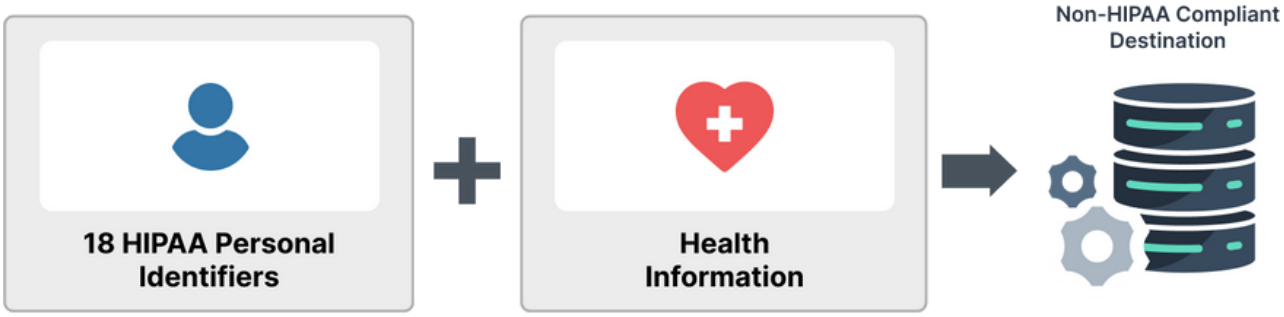
- To maximize conversions, Facebook needs to know the identities of the users who clicked on the ad and converted (who became new members in the example above). Facebook uses all the data points they have about the people behind those initial successful conversions to build a larger audience of users with similar traits. It's all very "black box," and it's hard to know what intersection points Facebook uses from campaign to campaign. The key thing to understand here is that the user's personal identifier is required to make this feedback loop work. That by itself isn't so much of an issue. But when combined with the next set of data, healthcare providers are at risk.

- When a Facebook user clicks an ad and lands on a healthcare provider's website, the Meta Pixel loads and captures as much data as possible. Most importantly, this can include URL names of pages visited, and actions taken – all of which could be potential examples of health information. If the Meta Pixel can see that a visitor navigated to a page on diabetes treatment, is that considered health information? Yes, it certainly is. These problems come down to the fact that you can't control the information sent to Facebook using the Pixel. The Pixel thinks it's at a smorgasbord, eating all the personal user data it can.

And if you're a healthcare provider, the two types of data that make up PHI you're concerned about Facebook having access to are:

- **Personal Identifiers**. This is any data that can reveal the actual identity of an individual. Facebook doesn't consider things like an IP address as PII, but HIPAA does, along with 17 other identifiers. The Meta Pixel captures IP addresses, device IDs, and even identifiers entered on form and submission pages.

- **Health Information.** This is the medical information about the user. Something as simple as visiting a find a doctor page or viewing a treatment page with a URL containing fibrolamellar carcinoma would be considered health information. The Meta Pixel captures the page names and actions across the site.



PHI is the combination of personal identifiers and health information

Any ad clicks originating from Facebook means Meta has the user's identity. And since the Pixel is capturing pages that user visits that potentially contain health information, sharing that data back to Facebook are a HIPAA violation. The most important thing to understand here is that PHI = Personal Identifiers AND Health Information. The violation happens when you share that combined dataset with a non-compliant destination like Facebook.

And if you're sitting there saying, "Well, I don't even use health information in Facebook campaigns," it doesn't matter. What matters is that the Facebook Pixel you loaded collects that data, and Meta is certainly using it.

In case you're thinking of a wait-and-see approach, none of this is speculation. Remember that investigation by The Markup that we mentioned? It found that PHI was being sent to Facebook servers by multiple major healthcare providers. That set off a series of events that has led to class action lawsuits, updates in the HIPAA guidelines, and ultimately FTC fines as high as $7.8M. There is a way forward, though. You can continue to use Facebook ads in a healthcare setting WITH maximize conversions as a bidding strategy. To do so, you need to:

1. Cut off Facebook's all you can eat approach to data by removing the Pixel
2. Block all health information from being shared with Facebook

Let's see how you do that.

How to make Facebook Ads HIPAA-compliant

By using the Pixel, your users' data is going from website -> Facebook directly. We need to remove the Pixel and use a platform like Freshpaint as a layer of data governance to severely limit the data that is sent to Facebook.

This website -> Freshpaint -> Facebook path means you can take advantage of Freshpaint's HIPAA compliance:

- **BAA For Full Protection.** Freshpaint signs a BAA and is purpose-built to collect, store, and manage sensitive data across your tech stack (Facebook does not sign BAAs).
- **Safe by Default.** Freshpaint's default state is to never send ANY data to non-compliant tools (Facebook's snippet sends all data by default vs. Freshpaint sends no data by default).
- **Server-Side Implementation.** Freshpaint is only implemented server-side to give you control over your data (Facebook's Pixel is installed client-side on a provider's website, giving facebook the ability to intercept identifiers, health information, and whatever data it wants).
- **Forced Allowlists.** By default, no data is sent to Facebook Ads. Instead, you choose the data and events you want to continue to send, eliminating the risk of accidentally sending PHI.

BOOK A DEMO

So what is the minimum dataset needed in order to use Facebook's maximize conversions performance goal?

Ad Click Attribution

Facebook has an ad click ID that attributes that a user clicked on a specific ad. Capturing that data point in Freshpaint and sending it back to Facebook helps you understand how to attribute visits. Which campaigns did they come from?

Conversion Tracking

Since you're trying to maximize conversions, you have a desired business goal. Earlier in this article, we discussed "new member sign-ups" as an example. Freshpaint can capture that successful conversion and share it back to Facebook. Since that conversion action also contains the ad click ID, Facebook can now attribute the original Facebook ad clicks with the business goal. Facebook knows that an ad click resulted in your business goal.

Maximizing New Conversions

That last piece revolves around "how do I find more users likely to click and convert?" This performance model relies on Facebook knowing who clicked and converted. Send Facebook a certain number of weekly conversions (many say 50, although I've seen this perform on much less), and Facebook will use its data to find the best possible audience. We've determined that an email or IP address is the best identifier.

If this part gives you pause and you're asking, "isn't sharing email or IP address with Facebook a HIPAA violation," let me remind you what PHI is in the first place. Earlier, we talked about Personal Identifier AND Health Information = PHI. Facebook needs identifiers to make the maximize conversion part of their product work. Facebook does NOT need any health information.

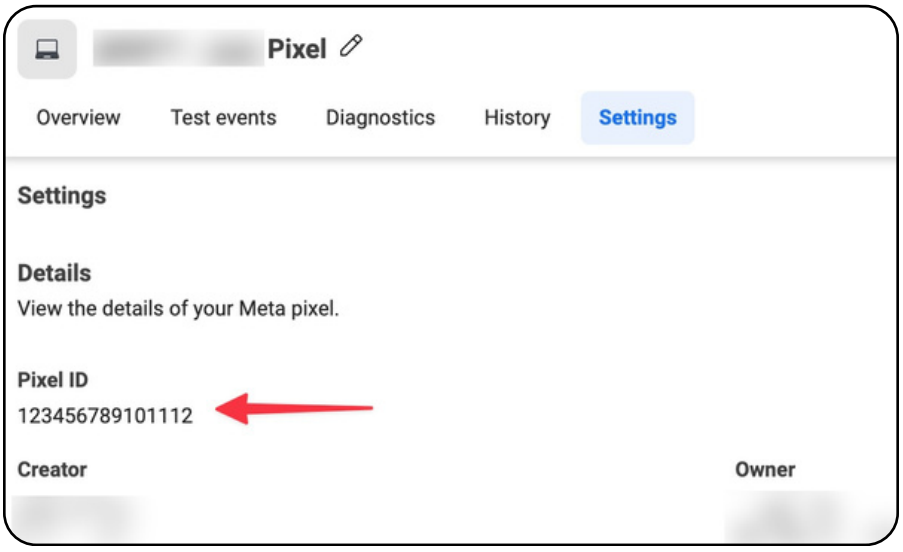
By removing the Pixel and using Freshpaint instead, advertisers can limit the data shared with Facebook to only the three things below.

Limiting the data shared with Facebook can keep you HIPAA-compliant while maintaining performance

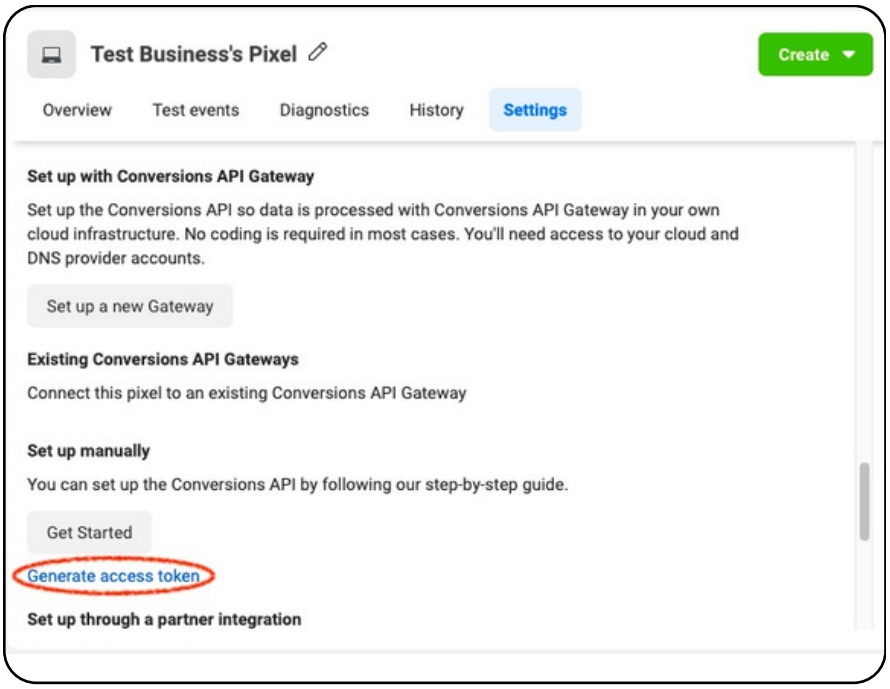
Freshpaint's approach allows you to continue leveraging your conversion tracking with Facebook Ads in a HIPAA-compliant way.

How to use Freshpaint to make Facebook Ads HIPAA-compliant

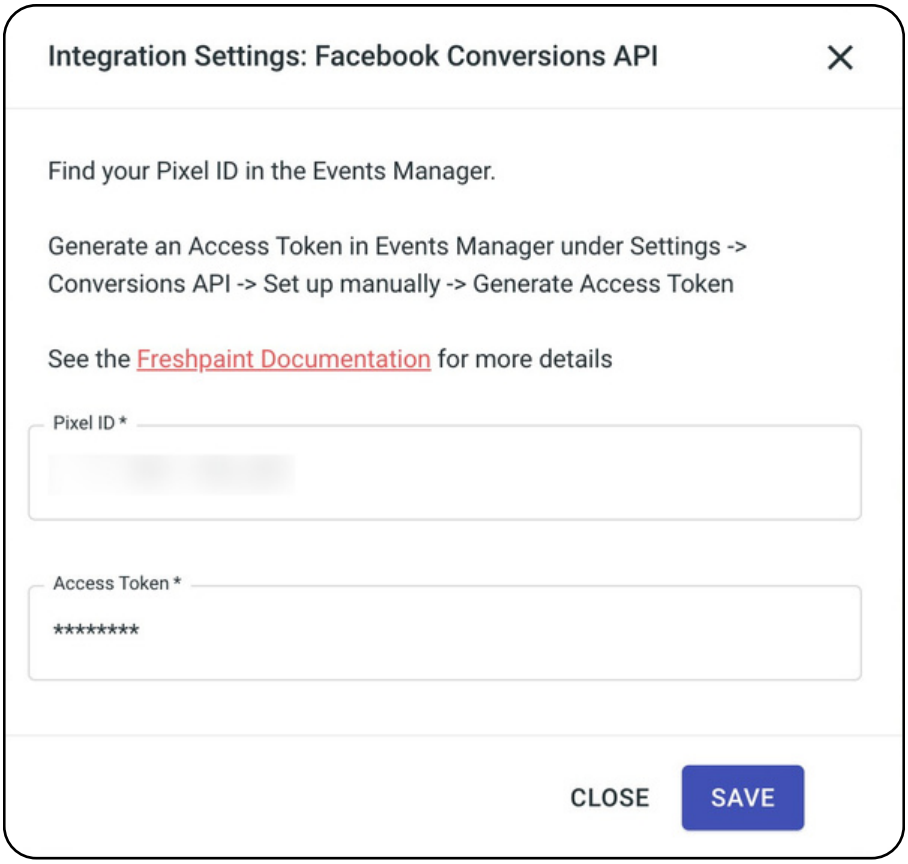
Here's how you can set that up in Freshpaint. We're going to need our Pixel ID from our events manager dashboard:



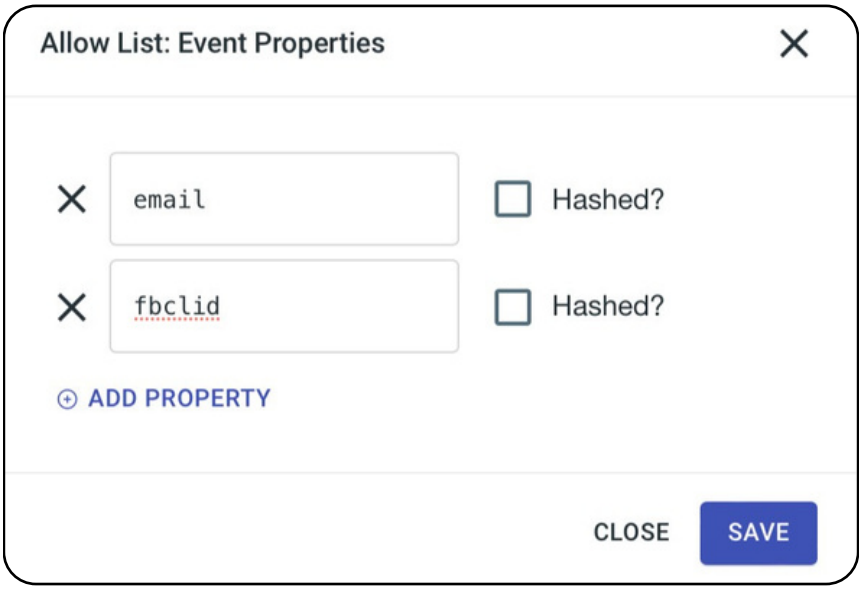
We'll also need to generate an access token in the same dashboard:



We'll add these to our Freshpaint Facebook Conversions API integration.

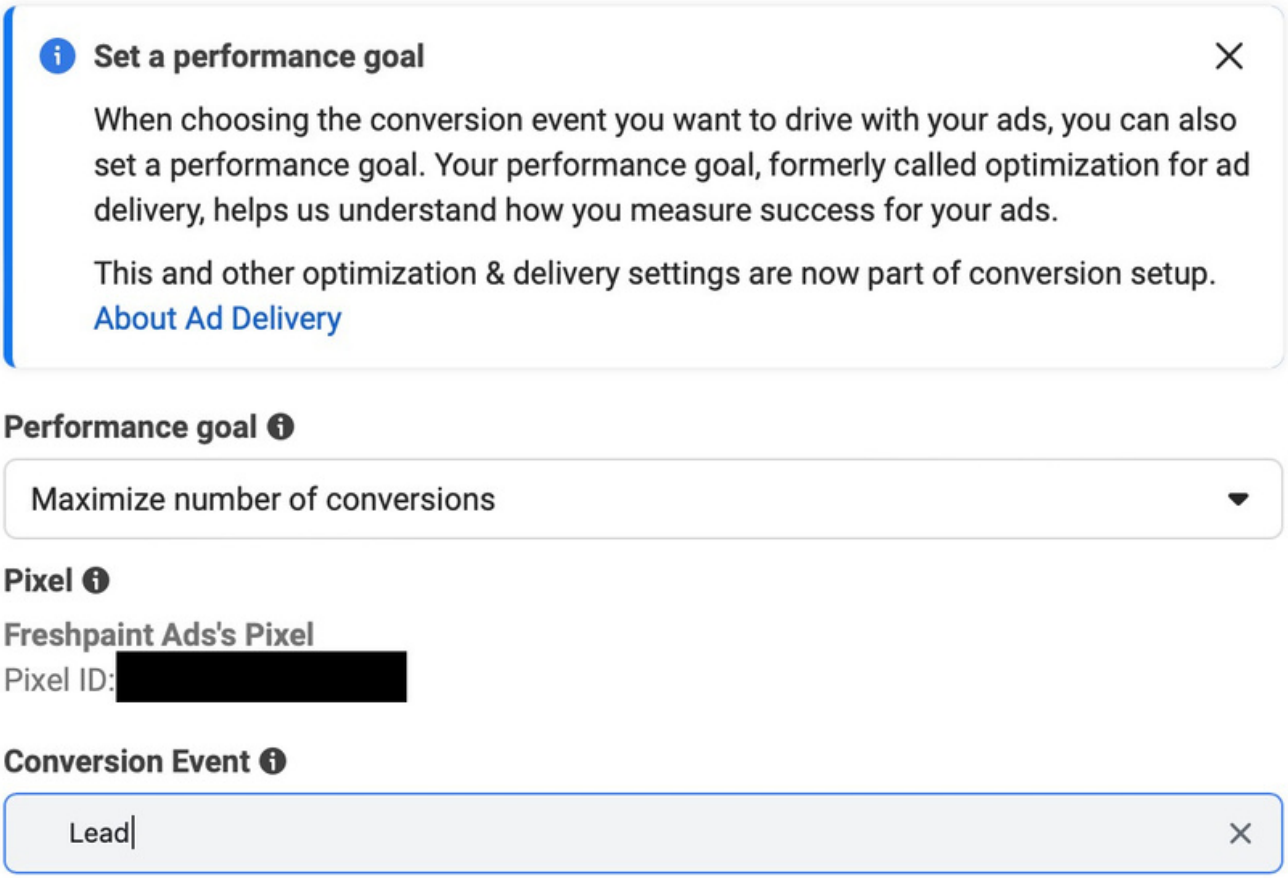


You then set the conversion events to share with Facebook. In HIPAA-mode, no data is sent by default. You must instead add the Facebook data you want to send to an enforced allowlist. For each event (the conversion action) we recommend sending the fbclid to handle the click attribution and the user email or IP address to handle the maximize conversions performance goal.



Finally, you need to add a Transformation to map your event to the standard Purchase or Lead event in Facebook. Facebook conversion tracking is set up to track a bunch of standard events, but you can map any event to this field and add a specific revenue amount if needed. Just be sure in naming conversion events that you don't share any health information with Facebook in the event name.

When you create your campaign in Facebook, you'll want to choose "maximize number of conversions" as your performance goal and choose the event you're mapping to like "lead" for the new member sign up example.



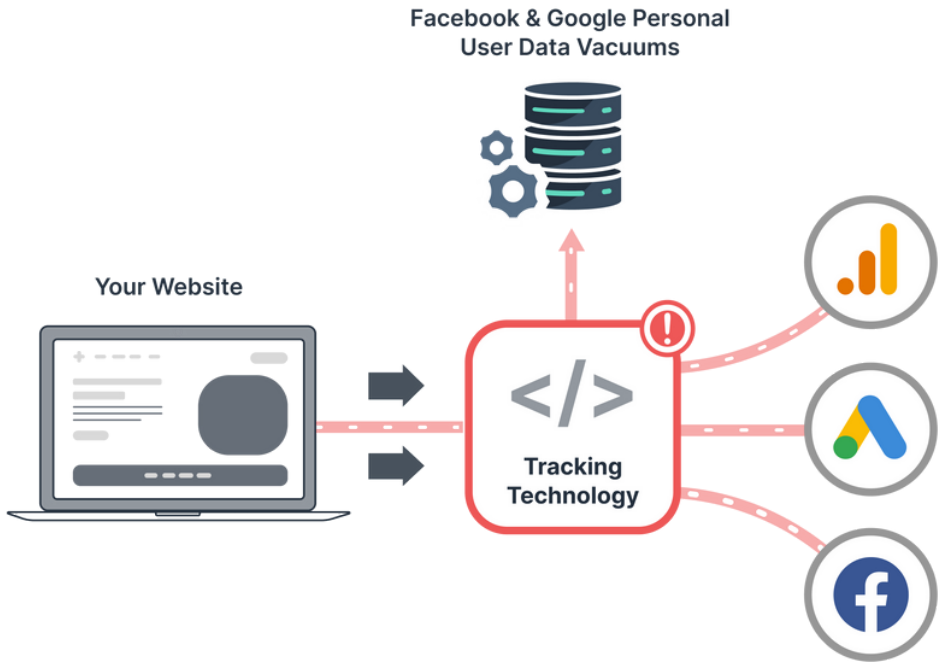
That's it. Conversion tracking is ready to go!

You still need to be careful about how you use this information. Having Freshpaint in the loop doesn't mitigate your role in making sure you are using patients, users, or visitors' data responsibly. What it does do is make it so you can use this data in conversion tracking to improve your Facebook Ads

How Freshpaint keeps you safe by default

Quick refresher: per HHS guidance, a HIPAA violation occurs when 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.

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



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

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.

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.

Freshpaint blocks personal information from being shared with Google Analytics

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 is 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

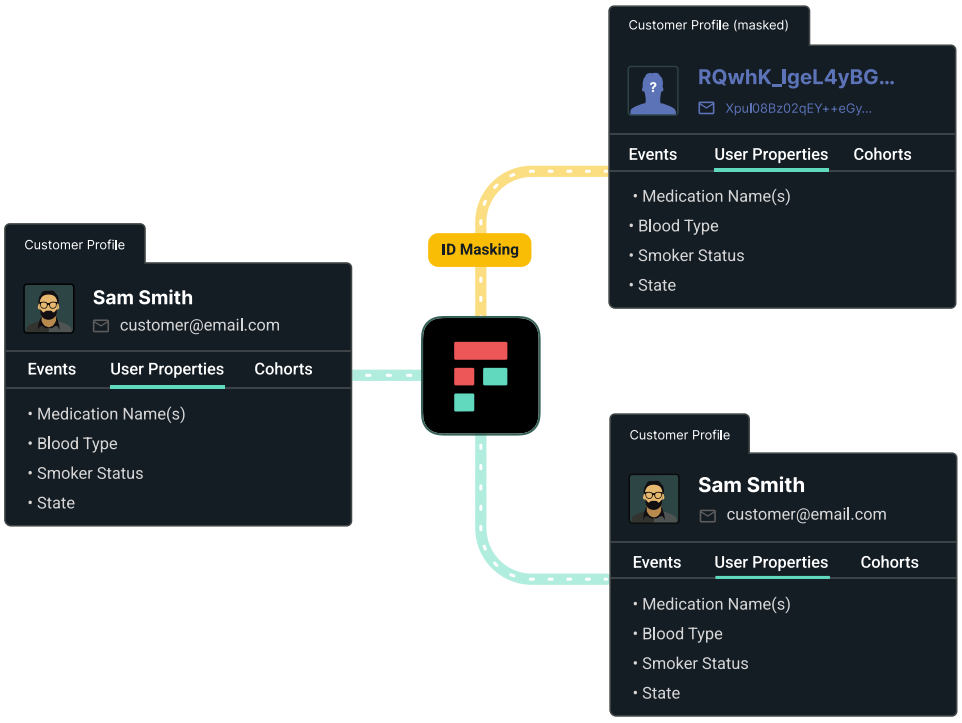
Instead of eliminating Google Analytics entirely, Freshpaint de-identifies users automatically. This way you can still connect all the points of the user's journey in GA without revealing who they are. Our ID Masking is HIPAA compliant. We do this by:

- Using cryptographic hashing
- Using a secret key
- Only sharing 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.



Freshpaint de-identifies users keeping you HIPAA compliant by default

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.

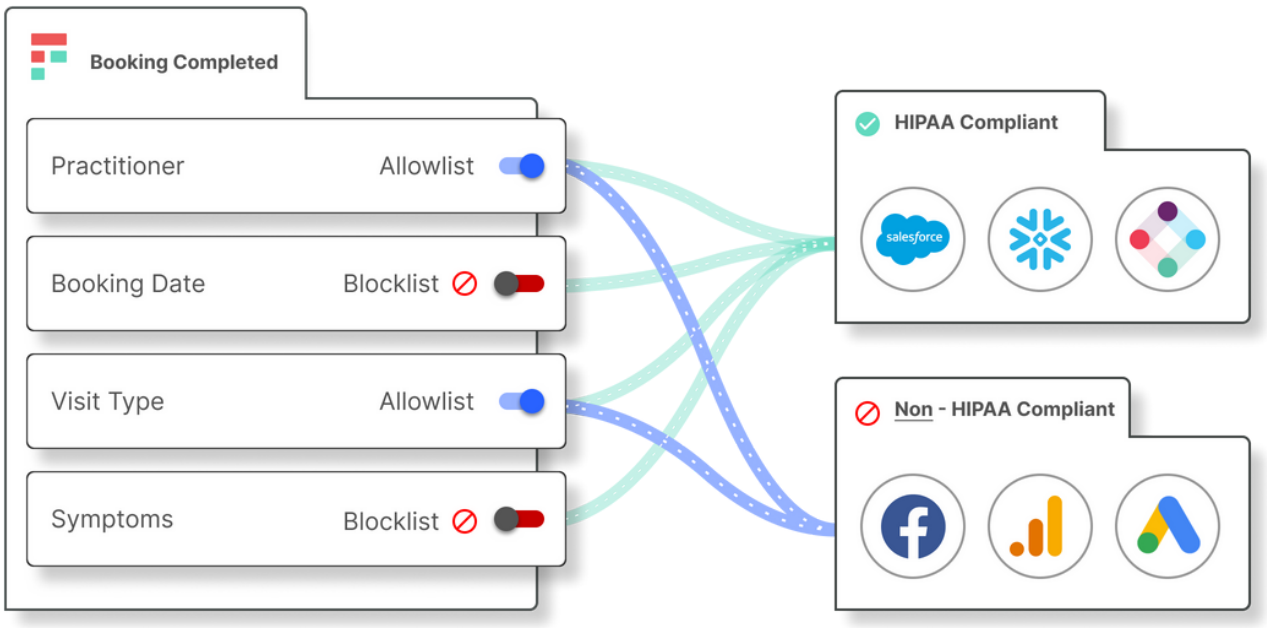
Enforced Allowlists

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 Forced Allowlists don't send any data to non-HIPAA compliant destinations by default

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.

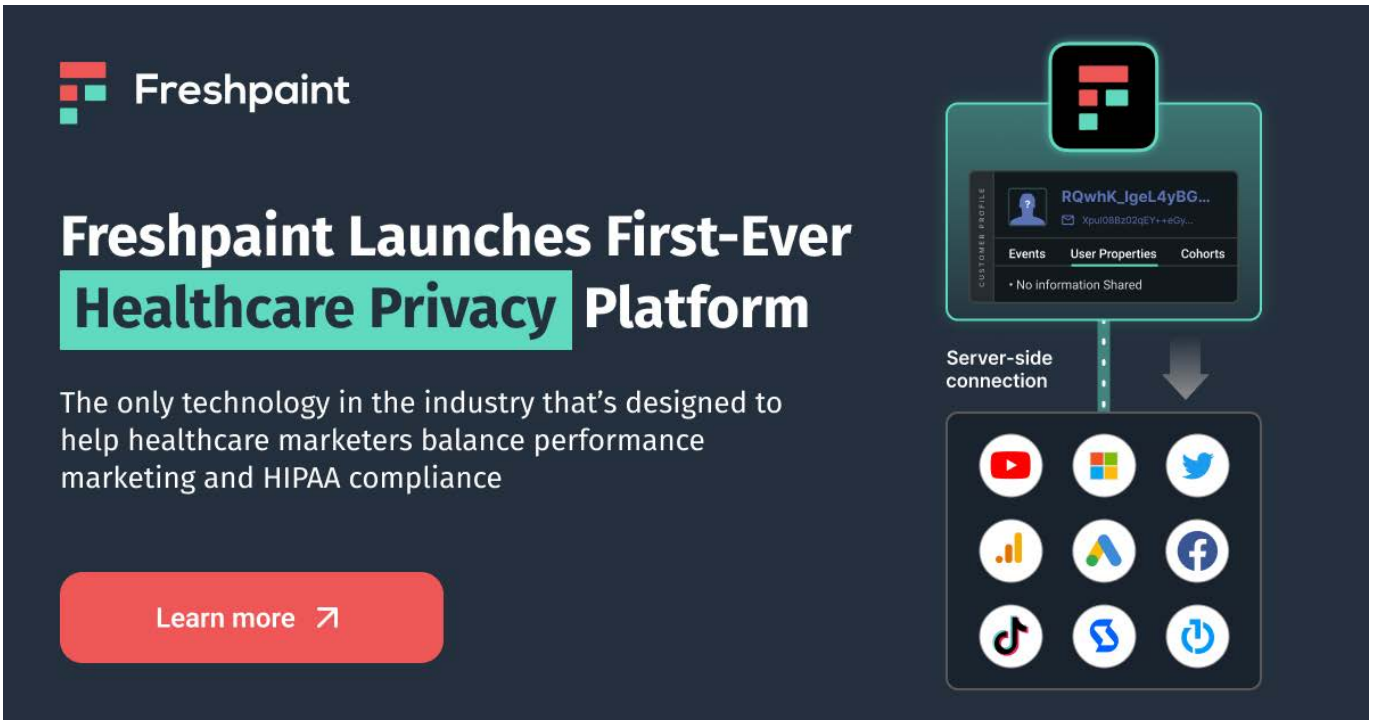
When you are making this choice, you have to look beyond the BAA. Vendors will say “yes, we sign BAAs” or “We’re set up to be HIPAA-compliant” but won’t go into the details. You have to press for the details.

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.

To learn more, visit freshpaint.io/hipaa



Freshpaint