Freshpaint

What CISOs Need to Know About HHS Guidelines on Tracking Technology & HIPAA

Freshpaint

CONTENTS

Freshpaint

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.

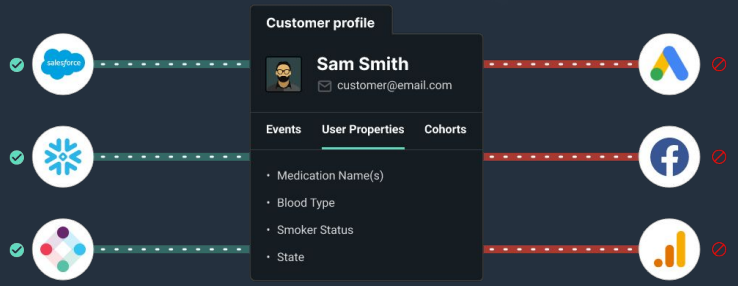
The original language of HIPAA couldn't have anticipated the complexities introduced by the revolutionary changes technology has brought to healthcare. To say we've been overdue for updated guidance from the US Department of Health and Human Services (HHS) is an understatement.

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?

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 explicitly calls 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 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).*

Freshpaint

Capturing customer data to improve product experience, provide more personalized messaging, or improve ad campaigns would all certainly be 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 review 2 common scenarios facing healthcare providers.

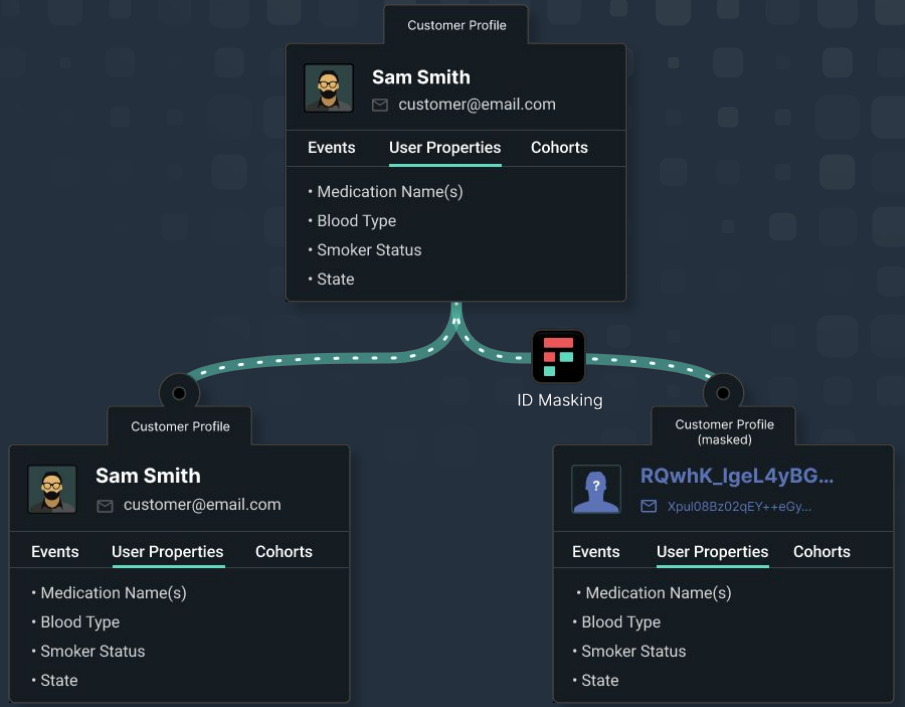
Freshpaint

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

The Google & 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 (Google Analytics at early stages and then graduate to Mixpanel, Amplitude, or similar)
- Session replay tools (CrazyEgg, HotJar)
- Chat tools (Drift, Intercom)
- Support tools (Freshdesk, Zendesk)
- 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.

Freshpaint

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.

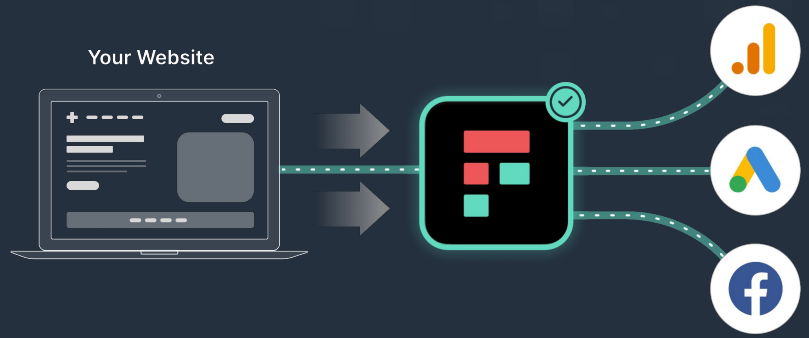
- What tracking technologies do we have in place?
- What tools need PHI to perform their function (like emailing appointment reminders)?
- Do we have a BAA in place with all of them?
- What tools don't need PHI to perform their function?
- How do we guarantee that PHI is never shared with those tools?
- 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.

This means 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.

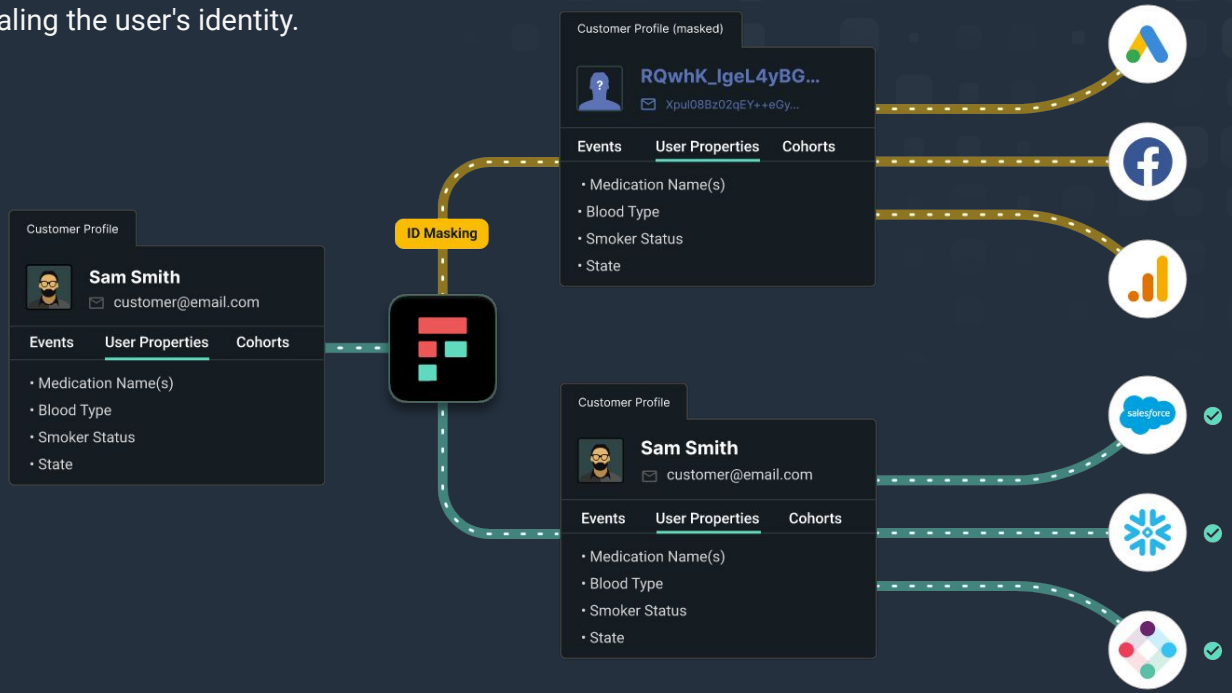


Freshpaint

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.



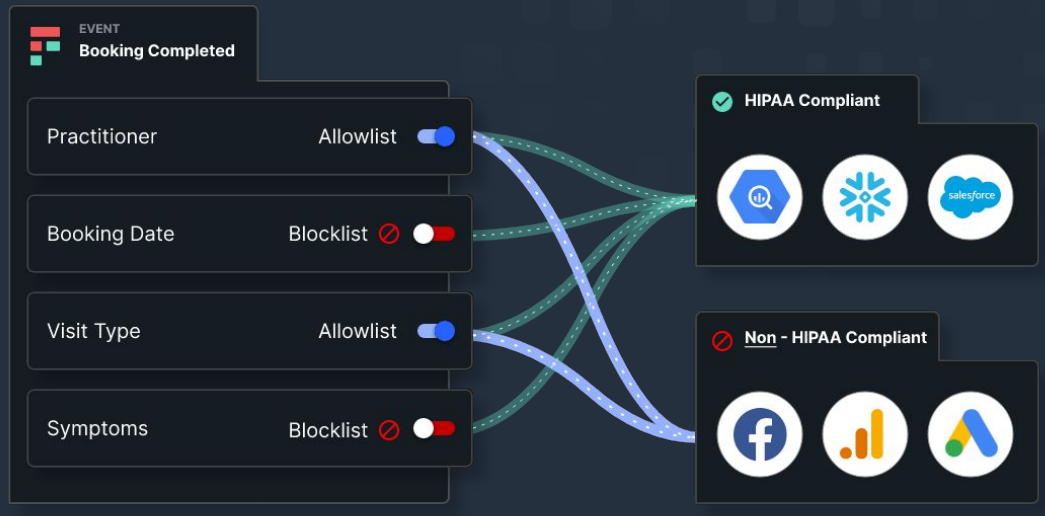
Freshpaint

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.



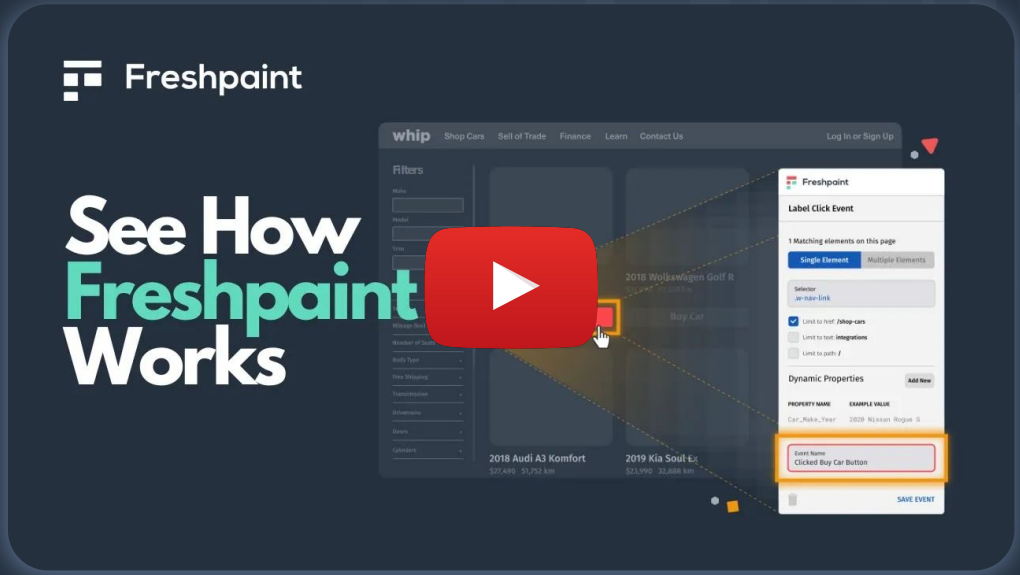
Freshpaint

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.

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.



Freshpaint

Ignorance is no longer an excuse: 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.

Freshpaint

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.

Freshpaint

June ‘22 - The Markup Investigation

Read the full story

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 ‘22 - Class action lawsuits against Meta

Read the full story

Two lawsuits were immediately filed against Meta.

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 site. 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 '22 - Northwestern lawsuit

Read the full story

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.

Freshpaint

He was seeking:

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

November '22 - WakeMed, Advocate Aurora, Duke, Northwestern class action lawsuit

Read the full story

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 '22 - HHS updates tracking technologies guidelines

Read the full guidance

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:

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.

Tracking within a patient portal is absolutely forbidden, no matter the intent.

You can read more about this HHS guidance here.

February ‘23 - FTC fines GoodRx $1.5M

Read the press release

By the start of this year, 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.”

Freshpaint

March ‘23 - FTC fines BetterHelp $7.8M

Read the press release

Which brings us up-to-date and 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.

Freshpaint

What will the rest of the year bring?

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. The FTC has made it clear they are coming for providers that run afoul of these regulations. Don't let that be you.

If you want to learn more about why tracking technologies could be tripping you up and what to do about it, download our comprehensive guide.

$1.5M fine issued by the FTC against GoodRx

Samuel Levine
FTC Director Bureau of Consumer Protection

"The FTC is serving notice that it will use all of its legal authority to protect American consumers' sensitive data from misuse and illegal exploitation."

Freshpaint

How Tracking Technologies Work, And Why They Violate HIPAA

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).

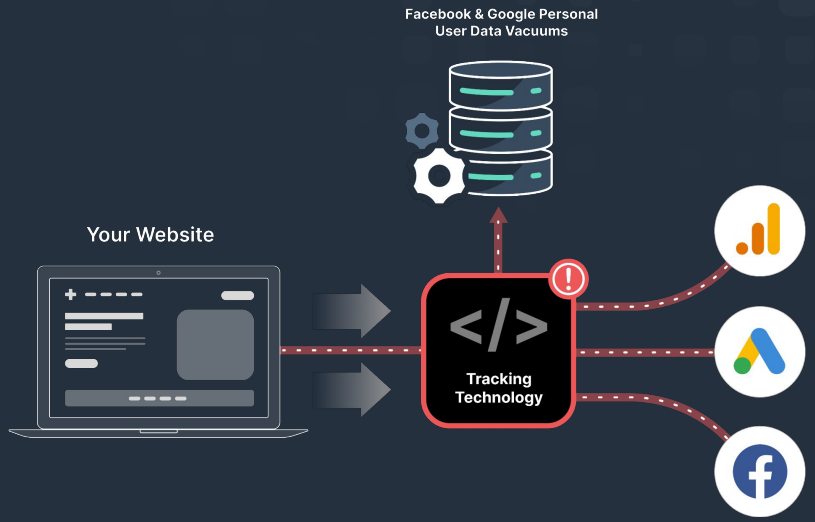
That “Individually identifiable” information is important in the context of tracking technologies. There are 18 individual identifiers in the HIPAA guidelines, including “name, address, birth date, Social Security Number,” but also including your IP address, device ID, or ZIP. These are all data points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

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:

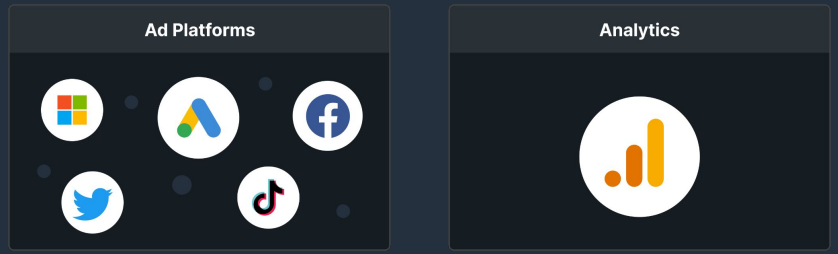
```
<noscript>
 <img height="1" width="1" style="display:none"

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.

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.

Freshpaint

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.

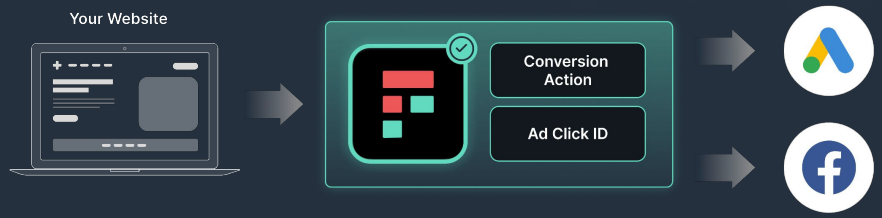
Freshpaint

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

Why Shutting Down Advertising Tracking Technologies is Impacting Your Marketing Team

When legal and compliance teams learn about the new HIPAA guidelines on tracking technologies, their direct message to their marketing teams is:

Turn this off. Now.

This is understandable. If you're using native Google or Facebook tracking, you will likely share HIPAA-protected data with non-compliant vendors. But what's also understandable is the frustration from the marketing team when they realize they have to remove them. That's because these technologies are vital to the success of their acquisition strategy. Suddenly switching off native trackers throws everything they are working on into chaos.

But the legal teams are right–as it stands, these native tracking technologies have gone from asset to liability. Marketers can't just walk away from these platforms, though. They need the data to find the right audience, generate leads at stable costs, and help grow their healthcare organization.

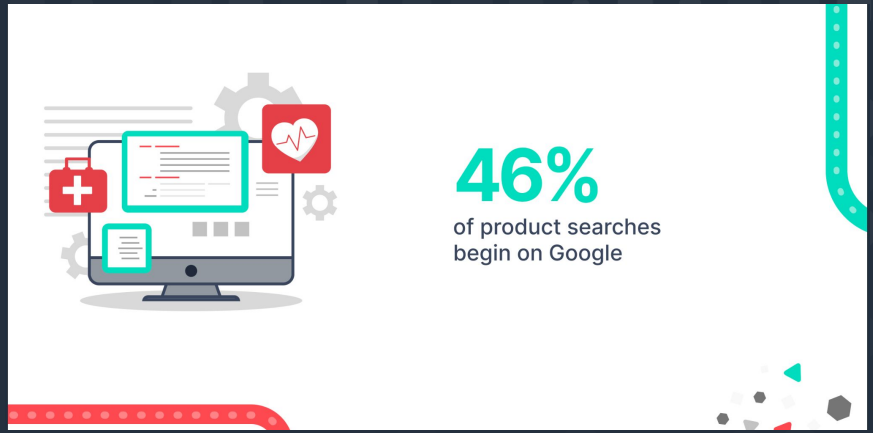
We will cover why your marketing teams rely on these platforms, how they are helping your company grow, and how legal and marketing can find the right balance between privacy and promotion.

Freshpaint

Why your marketing team relies on digital advertising channels to reach modern consumers

In marketing, you want to meet people where they are. In the modern world, that means the internet. 46% of product searches begin on Google. 72% of internet users in the US are actively engaged on Facebook. This is the main reason marketing teams want to use these channels–their ability to reach most of the consumer market.

In a market such as the US, people are always online–for work, entertainment, or random searching and scrolling. These channels are the first place most people will seek out information about healthcare information and services. By advertising on digital channels, marketers can reach patients and users where they are already spending their time.



With Google Search Ads, a marketing team can reach a vast audience by actively searching for specific keywords related to healthcare services.

Facebook Ads provides targeting options based on user interests, demographics, or behavior related to healthcare issues (such as searching for a support group or even being in an at-risk demographic).

Freshpaint

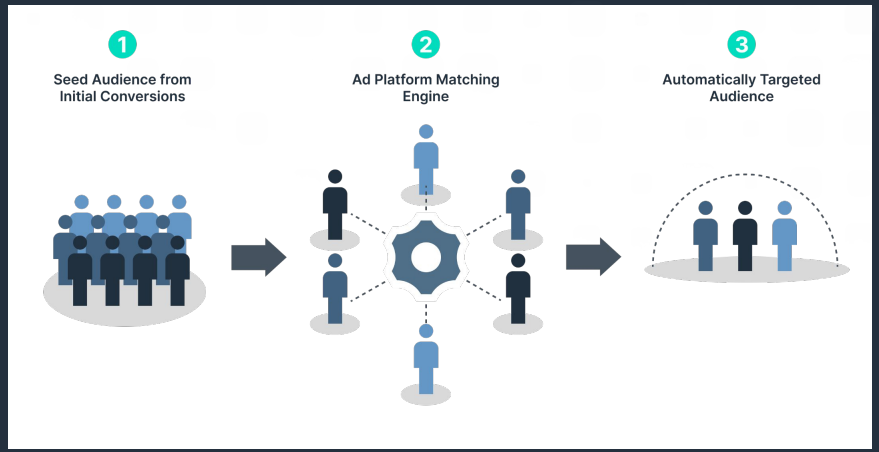
These channels are an effective lever for marketing teams tasked with driving the adoption of healthcare services. Your marketing team wants to:

1. Increase brand awareness, introduce your services to potential patients, and differentiate from competitors.
2. Capture leads in the form of scheduled appointments and new member sign-ups.
3. Ensure the cost for those leads is stable and aligns with the value of the services those consumers ultimately pay for.

How digital advertising channels use data to improve performance

Google and Facebook are powerful lead-generation tools. Both companies earn more than $100B annually thanks to precisely targeted advertising that produces high-quality leads at a highly predictable cost per lead.

Both advertising platforms ultimately help marketers generate more revenue because of the measurement and experimentation loops built in. When your marketing team releases an ad on Facebook or Google, they aren't just taking a shot in the dark–they are working within an experimentation loop that automatically works to continue improving those ads' targeting.



Freshpaint

Traditional media doesn't have the data feedback loops available to digital marketing. Digital advertising allows powerful machine learning models to continue optimizing so the right ad finds the right audience. Unlike traditional media, digital ad channels provide analytics, so your marketing team can measure key metrics like impressions, clicks, conversions, and return on ad spend (ROAS), providing insight into what's working and what's not.

Your marketing team sets up conversion tracking on the ads they put up on Google and Facebook. This means the platforms will track when a user performs a specific action, such as scheduling an appointment or becoming a member. By setting up this conversion tracking, marketers can measure the effectiveness of their ads and understand which ones are driving valuable customer actions.

But conversion tracking does much more than just measuring success. It helps drive that success. That's because both Google and Facebook use machine learning algorithms to analyze past conversion data and predict future conversion possibilities. These predictions inform automated bidding strategies, such as Google's Target CPA (Cost Per Acquisition) or Facebook's Conversion Optimization delivery option. These strategies automatically adjust bids in real time to prioritize showing your ads to people who are more likely to convert.

The final piece of the puzzle is who gets to see the ads. Facebook and Google can target new users who share characteristics with their existing converters. The platforms use machine learning to find patterns in the behaviors and characteristics of your converting users and then target new users who exhibit similar behaviors and characteristics.

Digital advertising platforms leverage conversion data to improve campaign performance, enhance audience targeting, and achieve better ad spend ROI.

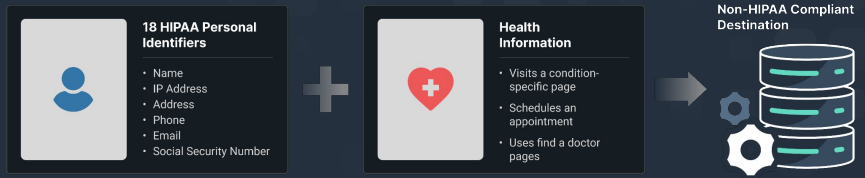
How HIPAA guidance negatively impacts advertising performance

What we've described so far is how almost every marketing team leverages digital advertising channels. To use those ad platforms effectively, you will use data and information about your users to better target ads to others that have the same behaviors online or fit in the same demographic.

But doing this using native tracking technologies is no longer an option for marketers in healthcare. As legal and compliance professionals, this line from the OCR guidance probably made you wince:

> *"This means that the platforms will track what a user does in response to an ad (e.g., click on it), and track them onto your website to see if they perform a conversion event, such as scheduling an appointment.*

The HIPAA guidelines on tracking technologies make it clear you cannot do this. Tracking a particular user making an appointment will be considered personal health information (PHI). The way Google and Facebook work is that they track what someone does on your website and several unique identifiers associated with that person, such as their IP address. This combination of the IP address as an identifier and health information like an appointment being scheduled is consistently tripping up healthcare marketers.



Identifiers AND health information are considered PHI

This is the problem when it comes to using the native tracking tools of Google and Facebook (and other platforms). Without necessarily knowing it, you are always sharing users' personally identifiable information with these platforms. They are not HIPAA compliant when coupled with health information because you can associate health information with a single individual.

Failure to comply with HIPAA regulations can result in significant penalties, including hefty fines and potential reputational damage. Each of these has already happened to numerous healthcare organizations over the past two years as federal regulators have started clamping down on HIPAA breaches.

Healthcare systems, ad platforms, and healthcare apps have all been sued or fined in the past two years.

How to restore the data feedback loop and also protect patient privacy

But there is a ray of hope for marketing and legal teams looking to strike a balance between privacy and promotion. Even though the native tracking technologies that power digital advertising tools like to capture as much information about your website visitors as possible, they don't need all of it to perform.

Native tracking technologies, by default, capture information like the names of web pages visited, the text on button clicks, and identifiers like IP addresses. But none of that information is required to run effective advertising on those platforms.

Ad platforms need a limited dataset to work effectively.

A better option for conversion tracking is to severely limit the data being shared to advertising platforms like Google and Facebook. Say your marketing team's goal is to capture leads in the form of visitors scheduling an appointment. Google and Facebook only need the Ad Click ID (from the native ad platform when the user clicks the ad), and a conversion happens. That conversion needs to be generically named (like "lead") so that it doesn't contain any health information.

By limiting the data set sent to Facebook/Google servers, you can avoid sharing PHI.

Freshpaint

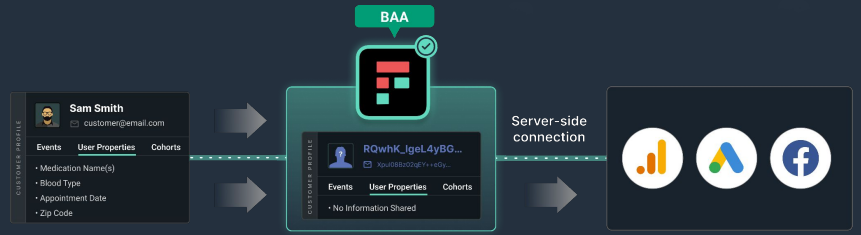
This is how Freshpaint can help healthcare marketing and legal teams run effective advertising campaigns while protecting patient privacy. Freshpaint replaces all native advertising tracking technologies and sits between your website and Facebook and Google Ads. Freshpaint helps keep consumer data safe by:

BAA For Full Protection. Freshpaint signs a BAA and is purpose-built to collect, store, and manage sensitive data across your tech stack (Facebook & Google do not sign BAAs for their ad platforms).

Safe by Default. Freshpaint's default state is never to send ANY data to non-compliant tools. This prevents things like IP addresses and health information from accidentally being shared. Healthcare marketing and legal teams must opt-in to send any data.

Forced Allowlists. You choose the data and events you want to continue to send through an easy-to-use user interface, eliminating the risk of accidentally sending PHI. By doing this through a UI vs. in the codebase, legal and compliance teams always have complete visibility to what data is being shared to which tool.

By using these practices, healthcare organizations can use digital advertising channels effectively while maintaining strict compliance with HIPAA regulations. It's a delicate balance, but with careful planning and execution, organizations can reach their target audiences, drive conversions, and avoid issues with the regulators.



Freshpaint keeps patient data safe by default.

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 safe by default

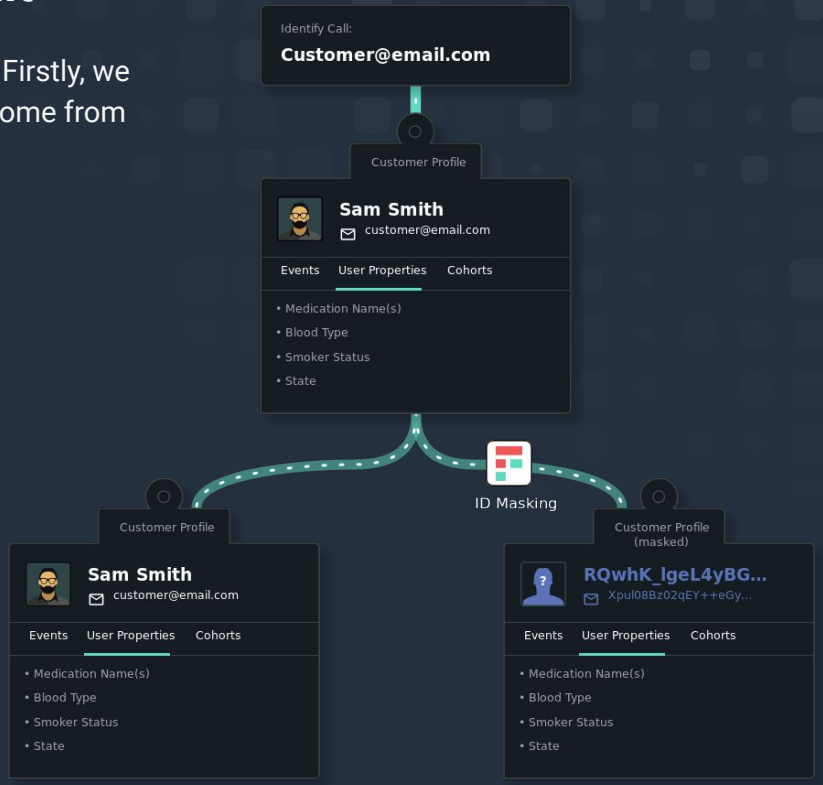
So there are three main components to how we work at Freshpaint. Firstly, we sign a BAA. But this is table stakes. Actual safety and compliance come from our ID Masking and our allowlist-first philosophy:

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

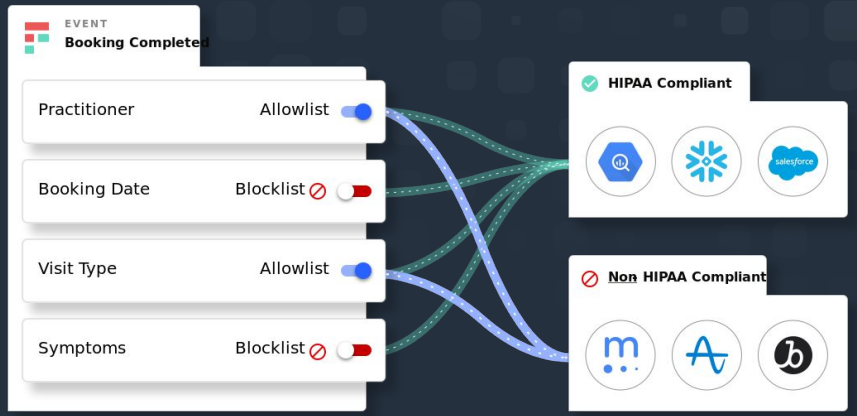
Choosing the right solution

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.



Freshpaint

Freshpaint's HIPAA-Compliant CDP vs Generic CDPs

In today's data-driven world, businesses constantly seek effective solutions to collect, manage, and analyze customer data to deliver personalized experiences. Customer Data Platforms (CDPs) have emerged as a crucial tool, allowing companies to unify and act on customer data from various sources.

But not all CDPs are created equal. Choosing the right platform becomes even more critical in industries where privacy and security are of utmost importance, such as healthcare.

HIPAA-Compliant CDPs help you execute your data-driven marketing strategies while complying with industry regulations. For healthcare providers, HIPAA-Compliant CDPs like Freshpaint have huge advantages over generic CDPs. If you're in healthcare, you'll want to read our breakdown of what to look for in a HIPAA-Compliant CDP.

HIPAA-Compliant CDPs are safe by default

The critical difference between a HIPAA-Compliant CDP and a generic CDP is the idea of "safe by default."

What does this mean? It starts with understanding that a CDP's job is to collect data from your website or product and share that data with your business tools. When those downstream tools aren't HIPAA-compliant, you suddenly have a problem.

To solve this, a safe by default CDP has features designed to keep the healthcare provider HIPAA-compliant and reduce their security footprint without needing custom engineering work.

To accomplish this, HIPAA-compliant CDPs must have several

layers of data governance to keep you safe. This is critical as generic CDPs will begin collecting and sharing data immediately after they are connected. If you are using a generic CDP, you can be out of compliance within seconds of turning the product on; with a "safe by default" CDP, you can easily control the data flow.

So what's required to be considered safe by default? Let's dive into it.

1) A Business Associate Agreement, or a BAA

“The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information.”

- HHS website

A BAA is table stakes for a HIPAA-compliant CDP. A BAA states all the processes and procedures a company has in place to "appropriately safeguard protected health information."

At Freshpaint, our BAA states we can safely collect and store data collected about the actions visitors take on a healthcare provider's website or in their products.

Freshpaint

A BAA is a must-have component of a HIPAA-compliant CDP, but it's not enough. That's because while the BAA makes sure your CDP can safely collect and store data, it does not make you safe when sharing your data with tools that are not HIPAA-compliant. You'll need a lot more to make tools like Google Analytics and ad platforms that are not HIPAA-compliant safe.

2) Strong PHI Governance

The BAA is just the legal obligation. HIPAA-compliant CDPs need actual engineered safeguards in place to ensure strong PHI governance so they don’t run afoul of regulators. CDPs ultimately send data to other destinations. So if you’re sending ungoverned data to a non-compliant tool like Google Analytics, the BAA you signed with your CDP isn’t really all that useful, is it?

At Freshpaint we have three components to ensure strong PHI governance.

ID Masking

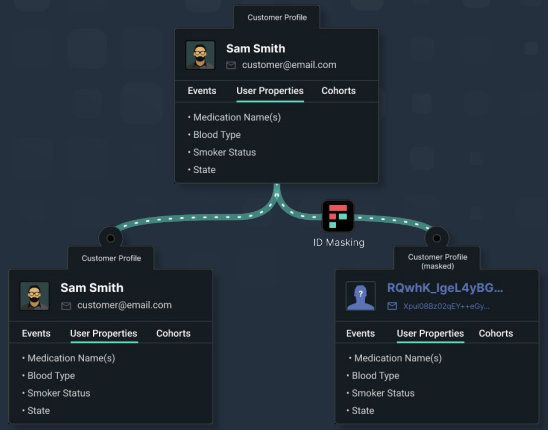
Modern marketers are looking for a complete view of the customer journey. Modern marketing tools give them just that. By tracking individuals across sessions, you can see how a person is interacting with your site or your brand across days and weeks.

To do so, they need a way to identify individual users. This might be email addresses if they are logged into a site, or an IP address if they aren't. But in healthcare you need to protect the visitor's privacy and do it in a way that never reveals the identity of that visitor.

These two options seem entirely contradictory. But you can both track across sessions and respect privacy through ID masking. Freshpaint automatically masks the identity of visitors in a way that never reveals their identity to tools like Google Analytics (This is called de-identification and how HIPAA wants you to deal with identifiable information).

To be considered HIPAA-compliant ID Masking, Freshpaint cryptographically hashes all user identifiers server-side using a secret so that the hash is entirely irreversible. Most generic

CDPs don't do cryptographic hashing, but if they do, it's client-side without a secret. Client-side without a secret doesn't follow the HIPAA de-identification standards and is reversible, so it will still put you at risk.



Freshpaint de-identifies visitor data in a way that meets the HIPAA standards

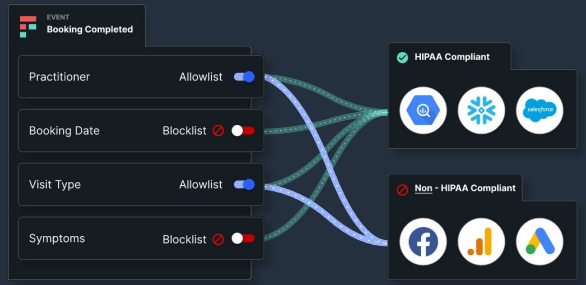
For generic CDPs that don't do cryptographic hashing, your engineering team will have to create a custom anonymizing function before you send the data to the CDP. Building an anonymizing function is a heavy lift for healthcare providers.

Freshpaint

Forced Allowlists

As we said above, a generic CDP automatically starts sharing data downstream when you switch it on. For healthcare organizations, that means that identifiers like IP addresses that are in the metadata can be inadvertently shared with tools that are not HIPAA-compliant.

Freshpaint solves this by providing a forced allowlist through a user interface where legal and security teams can select which data is shared and have a single view of which data is shared.



Freshpaint offers full control over which data is shared with each destination.

The default setting is that no data is flowing to downstream tools that are not HIPAA-compliant. You control all data flow from your site or product through a single centralized place that forces an opt-in approach to what data can go to which destination.

Role-Based Access Control

The last component of strong PHI governance is good access control. Often with CDPs, analysts or engineers can turn on (or off) any data flow they need. Again, this is built with ease of use rather than security in mind.

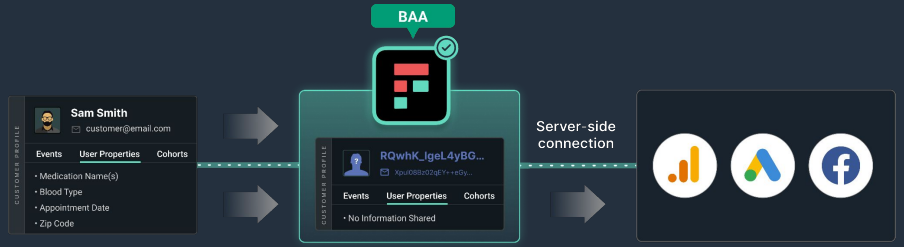
But in sensitive areas like healthcare, legal and security teams want a way to restrict the ability of team members to change settings that allow new data to flow freely to downstream tools.

Role-based access control (RBAC) provides your legal team with final approval to share any new data. This helps avoid accidentally sharing PHI with non-compliant tools.

3) Enhanced Server-Side Connections

Most native tracking pixels use client-side tracking. Native pixels load on the visitor's computer when they visit a hospital website and give you the wealth of information you need for using ad platforms and analytics. But when those pixels load client-side, they also have access to personal identifiers like IP addresses and health information like the page URL.

To cut analytics and ad platforms off from access to PHI, HIPAA-compliant tracking requires server-side connections to be safe. The standard server-side destinations of generic CDPs don't provide the same data and functionality as the client-side native pixels, rendering your downstream tools useless. They may make you safe but won't feed those tools with the data you rely on for your analysis.



Freshpaint uses enhanced server-side connections for full functionality of destinations.

Freshpaint has designed a novel form of server-side integration called a proxy integration. Freshpaint's proxy integrations emulate the client-side integration but run on Freshpaint's servers instead. The proxy integration provides the same functionality as if the native tracking pixel was installed directly on your site but without the risk of exposing PHI to non-compliant destinations.

4) 2 Week Implementation

The final part of moving to a HIPAA-compliant CDP is implementation time. If the move to compliance is difficult, people will put it off. As it stands, most healthcare marketing teams rely on Google Tag Manager to handle their events.

Freshpaint makes it easy to take your existing tags from Google Tag Manager and route them through Freshpaint instead of directly to tools like Facebook and Google Analytics. This allows teams to implement Freshpaint in two weeks or less.

For healthcare providers looking to move away from Google Tag Manager, Freshpaint offers an easy-to-use event management platform and a white glove service to migrate to it.

Freshpaint

Freshpaint is built for healthcare providers

If you're dealing with sensitive data in a healthcare setting, a HIPAA-compliant CDP is a must. It will power the tools you need to achieve your growth goals while keeping you out of the news, off the wall of shame, and clear of lawsuits.

Freshpaint is engineered to make it easy for the marketing teams at healthcare organizations to continue working with the analytics and ad platforms they rely on to promote their services. You can still get all the data and functionality you need, but with the benefit of peace of mind knowing that the data of your visitors or users is secured.

If you're in healthcare, you need a HIPAA-compliant CDP—which includes much more than a BAA. That's because safe by default means having a CDP with built-in data governance, automated de-identification, robust server-side connections, and quick implementation. For healthcare providers, a HIPAA-compliant CDP such as Freshpaint is the best path forward.

two chairs

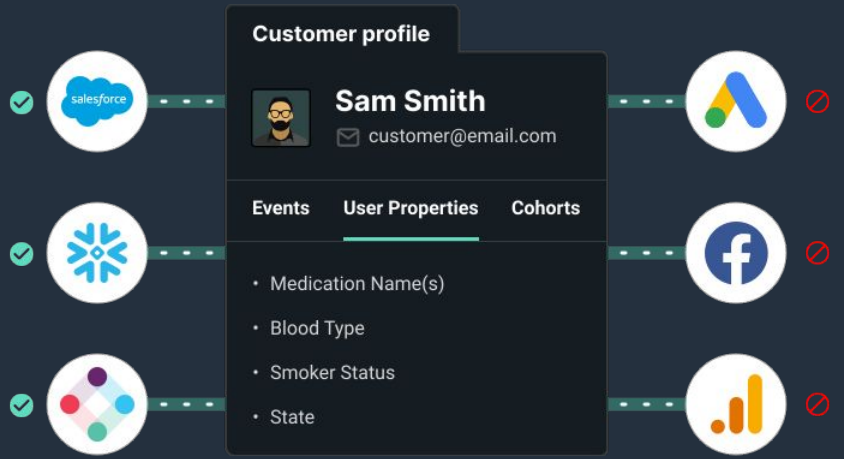
*"The killer thing about Freshpaint is the ability to control the flow of PHI to various destinations is a **super powerful unlock**."*

Scotty Abramson
Director of Growth

Take the Next Step with Freshpaint

Ignoring HHS's latest guidelines on keeping your first-party customer data HIPAA compliant isn't an option. But managing it on your own opens you up to significant engineering investment, human error, and an ever-expanding security footprint.

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.



Freshpaint

Meet with one of our experts →