Freshpaint

HIPAA Hazards:

Exploring Web Trackers Beyond Google Analytics

A Guide to Identifying and Resolving Web Tracker Risk for High Performance, HIPAA-Compliant Marketing

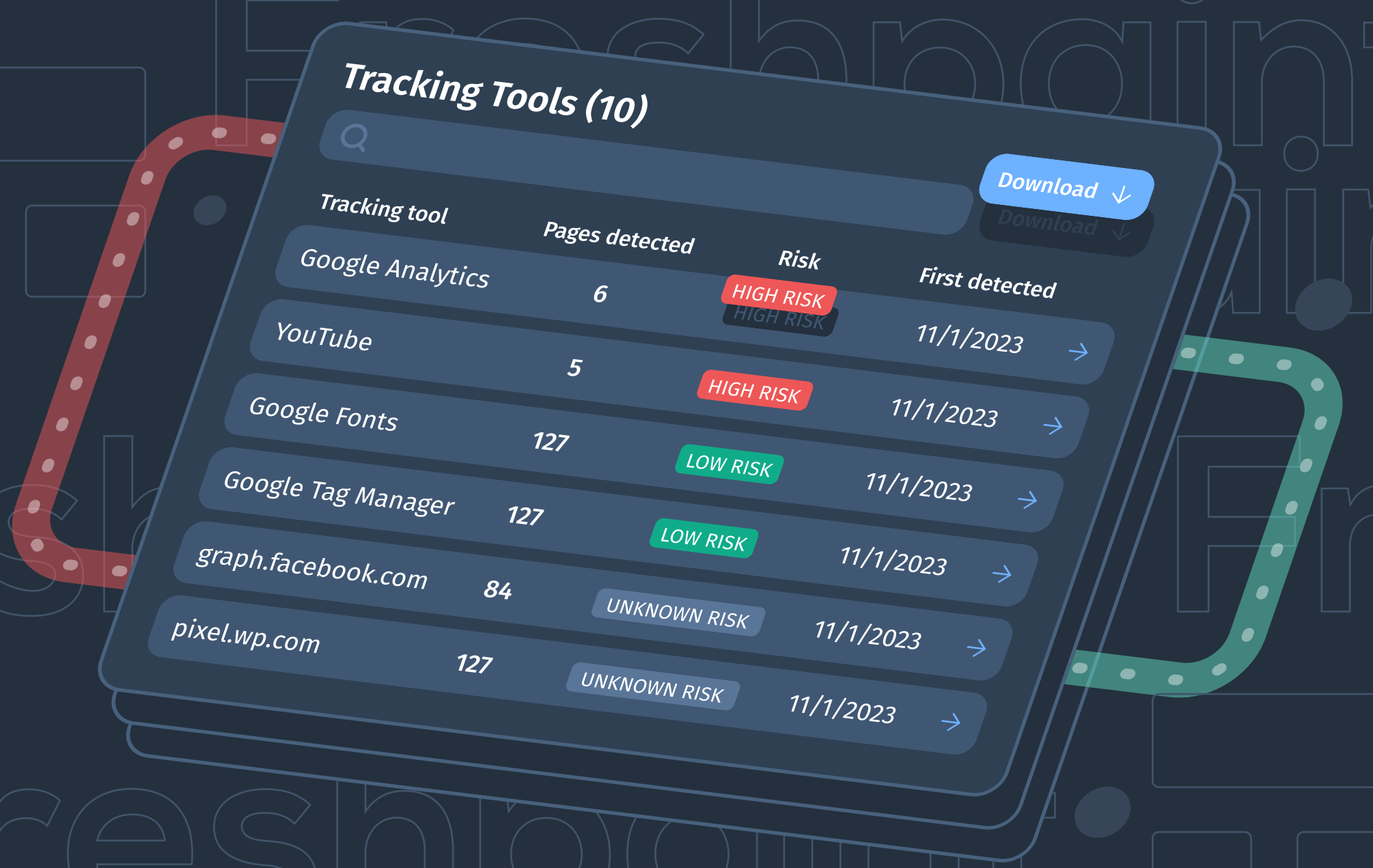


Table of Contents

Introduction

In 2023, when **HHS and the FTC** warned healthcare organizations about web trackers, all eyes were on Google Analytics and the Meta Pixel. Because the regulators explicitly called them out.

But these aren't the only web trackers that could compromise your HIPAA compliance. Any tracker that collects health information and personal identifiers puts you at risk of violating HIPAA. Those two components – health information and personal identifiers – are considered Protected Health Information (PHI).

And to be clear, all web trackers have access to **IP addresses**, which HHS has said is a personal identifier. So, every single web tracker on your website is already halfway to collecting PHI.

That means any web tracker that also collects the other half of PHI, health information, puts you at risk of HIPAA violations. And there are a lot of web trackers that collect health information. Any web tracker on a healthcare website that captures page visits, videos viewed, appointment information, medication data, or a whole host of other data is collecting health information.
You can see how this list of risky web trackers grows quickly. It's this ever-growing list of trackers that has led to **multiple fines and lawsuits** against healthcare organizations like:

- Advocate Aurora Health
- GoodRx
- Cedars-Sinai Medical Center
- New York-Presbyterian Hospital

To help you understand all of these web trackers, and what to do about them, we put together this guide. In it, we cover four types of web trackers that you might have on your website, what they mean for HIPAA compliance, and what you can do about them. (Hint: It doesn't involve removing all trackers from your site.)

1. Analytics Trackers

You'd be hard-pressed to find a marketing team in any industry, including healthcare, that doesn't use some kind of analytics tracker. Without them, it's impossible to measure how many people come to your website, which pages they visit, whether they convert, and all sorts of other useful information the marketing department needs to measure performance.

Unfortunately, analytics trackers tend to be major culprits for HIPAA violations, causing healthcare marketers all kinds of headaches. Below, we look at the most common ones.

Google Analytics

Google Analytics (GA) is the most popular choice for measuring website performance, and as you might already know, poses a huge risk to HIPAA compliance.

The Google Analytics tracker is one of the trackers that prompted **HHS to publish guidance** about the use of online tracking technology. It's also the tracker that has caused **multiple fines and lawsuits** against healthcare organizations.

The reason Google Analytics is risky is simple. The GA tracker collects both personal identifiers, like **IP address**, and health information based on the pages website visitors view. If that's not risky enough, Google won't sign a **Business Associate Agreement (BAA)** with any organization.

Even though GA doesn't store this data, the HHS guidance is clear: without a BAA, sharing personal identifiers with third-party trackers could still lead to a HIPAA violation.

Adobe Analytics

Abobe Analytics is a commonly used enterprise analytics platform. Unfortunately, for large healthcare organizations using it, it is not HIPAA-compliant out of the box.

The Adobe Analytics tracker works in a similar manner to Google Analytics. It collects page views, events, and identification data about website visitors. Any of those components are considered PHI, which puts healthcare organizations using Adobe Analytics at risk for HIPAA violations.

If that's not enough risk, Adobe doesn't actually consider its analytics platform to be a **HIPAA-ready product.**

Other Risky Analytics Trackers

Google Analytics and Adobe Analytics aren't the only analytics trackers that could put you at risk for HIPAA violations. Any analytics tracker that collects both visitor information and pageview or event information is a risk.

And since all analytics trackers collect that information, popular tools like Mixpanel, Amplitude, Hotjar, HubSpot, and so many others could put your organization at-risk.

How to De-Risk These Trackers

You have three options to de-risk these web analytics tools:

1. Put a BAA in place with each tool.
2. If you cannot get a BAA in place, use a **Healthcare Privacy Platform** to govern the flow of data to that tool. This will prevent PHI from being inadvertently shared with the analytics tool.
3. If you cannot do either of those, you have to remove the tracker from your website and stop using that analytics tool.

Fortunately, option three is rarely a reality for most healthcare marketers who want to use analytics tools. Options one and two are much more likely to solve the analytics headache.

2. Ad Trackers

Advertising trackers measure the impact of your marketing campaigns. They track what kind of actions a specific visitor performs on your website after seeing an ad. That information helps with remarketing, advertising efficiency, and driving down the cost of acquiring patients through ads.

And, much like analytics trackers, ad trackers cause a whole host of HIPAA headaches for healthcare marketers.

Google Ads

Google Ads trackers typically appear as “googleads.g.doubleclick.net” or “static.doubleclick.net” in the source code of your website.

These tracking tools monitor specific user actions to improve advertising effectiveness. For example, if you’re trying to use Google Ads to increase the number of "appointments booked," the..

tracker identifies website visitors who clicked on a Google ad and subsequently booked an appointment. This data helps in targeting ads more effectively by identifying and reaching out to potential patients who are also likely to book an appointment.

This process involves collecting both health information and personal identifiers, which are the two components of PHI and therefore put you at a high risk of violating HIPAA.

Meta Pixel

The Meta Pixel (also known as the Facebook Pixel) tracks the actions of Facebook and Instagram users. Like Google Ads, the Pixel measures ad performance. You can also target specific audience groups with ads based on actions they took or content they viewed on your website.

As the HHS letter says, the **Meta Pixel isn't HIPAA compliant.** In fact, it has led to **multiple fines and lawsuits** between healthcare organizations and patients who had their privacy breached.

Microsoft Ads

Microsoft's Ads platform, which powers ads on Bing, operates in the exact same way as Google's ads tracker.

That means the exact same risks exist for healthcare organizations using Bing and its web tracker as those using Google Ads.

Programmatic Ads

Programmatic Ad platforms pose a risk to HIPAA compliance because they use trackers and pixels to better understand visitor behavior. The Trade Desk and StackAdapt are two of the most popular programmatic ad platforms, each of which have trackers that help to enable remarketing and view-through conversions.

When someone views an ad where you're using a view-through conversion, the ad platform sends a cookie to the ad viewer's device and notes it with the tracking pixel.

If the ad viewer later visits your website and completes a conversion action (like scheduling an appointment), the tracking pixel logs that action and checks to see if there is a cookie on the visitor's device. If there is a cookie, the tracking pixel logs that, too. Then, it stitches everything together to tell the marketer a view-through conversion has taken place.

On top of that, these trackers sometimes load additional advertising pixels onto your website, so other platforms can run retargeting campaigns on behalf of a programmatic platform. This means your visitor data (including PHI) is shared with even more third parties.

How to De-Risk These Trackers

It's highly unlikely that you'll be able to sign a BAA with any of these platforms because they operate on a "more data is best" model – meaning they ingest as much data as they can to help with ad performance optimization. BAAs prevent these tools from ingesting as much data as possible.

Your only option for these trackers is to replace them with a Healthcare Privacy Platform to govern the flow of data to the ad platforms.

3. Embedded Video Trackers

Numerous healthcare organizations embed videos on their websites to improve their patient experience. But embedded videos also come with trackers that may put HIPAA compliance at risk.

YouTube Trackers

YouTube is owned by Alphabet, Google's parent company. So you can already imagine their user data collection capabilities are as robust as GA's.

When someone watches a video on your website, YouTube will receive the viewer's location data. Along with that, YouTube creates transcriptions of each video, meaning Google has health context of the embedded video. Location data and health context are two components of PHI, which puts you at-risk for HIPAA violations.

The video will also be added to the viewer's watch history, which the platform uses to personalize ads and content recommendations. This raises a red flag for HIPAA compliance.

Vimeo Trackers

Like YouTube, Vimeo also gathers a lot of data on their viewers.

When you embed a Vimeo player on your website, the tracker will collect data such as the user's IP address, operating system, and device and browser type.

If your embedded videos also contain health information, then you're sharing PHI with Vimeo.

How to De-Risk These Trackers

You could stop using embedded videos on your website altogether, but it's a user experience tradeoff. Embedded videos often provide a great user experience for your website visitors. On top of that, finding all of the embedded videos on your website and taking them down is a long, arduous process.

The other option would be to use a Healthcare Privacy Platform to help govern the flow of data to YouTube and Vimeo.

4. Embedded Maps Trackers

Embedding a virtual map on your website helps patients quickly get directions to your location. But to get directions, the user has to share their own location, which exposes you to a potential HIPAA violation.

Google Maps Trackers

Google Maps is by far the most widely used embedded mapping tool. If you want website visitors to easily find your locations, chances are you're using Google Maps.

But, like other tools in the Alphabet family, the Google Maps tracker collects plenty of user data. Embedding Maps onto your website gives Google access to user locations, which is a personal identifier. Health information is only a click away and is shared with Google Maps through a scheduling feature or through health information on a page.

How to De-Risk These Trackers

You only have a few options here:

1. Use another mapping tool that will sign a BAA.
2. Stop using mapping tools on your website, but this is a user experience tradeoff.
3. Use a Healthcare Privacy Platform that has mapping functionality built in.

How To Find Third-party Trackers On Your Website

The average health website has **15 web trackers**. But the number could be a lot higher depending on the size of your website.

The first step to finding third-party trackers is to do a **full audit of your website**.

According to Bridget O'Connor, Partner and Chief Operating Officer at Fortalice, this means compiling a list of all the pages associated with your domain.

"Once we get that inventory, you need to find out what trackers are on those pages," explains O'Connor.

At this stage, you have two options: find trackers manually by checking each page or using an automated tool that'll do the heavy lifting.

Or, use Freshpaint's **Web Tracking Monitoring** tool to scan your entire website and create a report that lists each tracker, as well as its location on your website.

Each detected tracker will come with a risk score so you can quickly take the appropriate action to mitigate any compliance risks.

Which brings us to the next section.

You Found The Trackers – Now What?

Many healthcare companies had a knee-jerk reaction when the HHS and FTC letter came out. **Deleting all trackers** seemed like the safest option.

But if you remove all trackers, the entire organization will lose out on valuable customer insights. Instead, you can make these trackers HIPAA compliant by using a Healthcare Privacy Platform like Freshpaint.

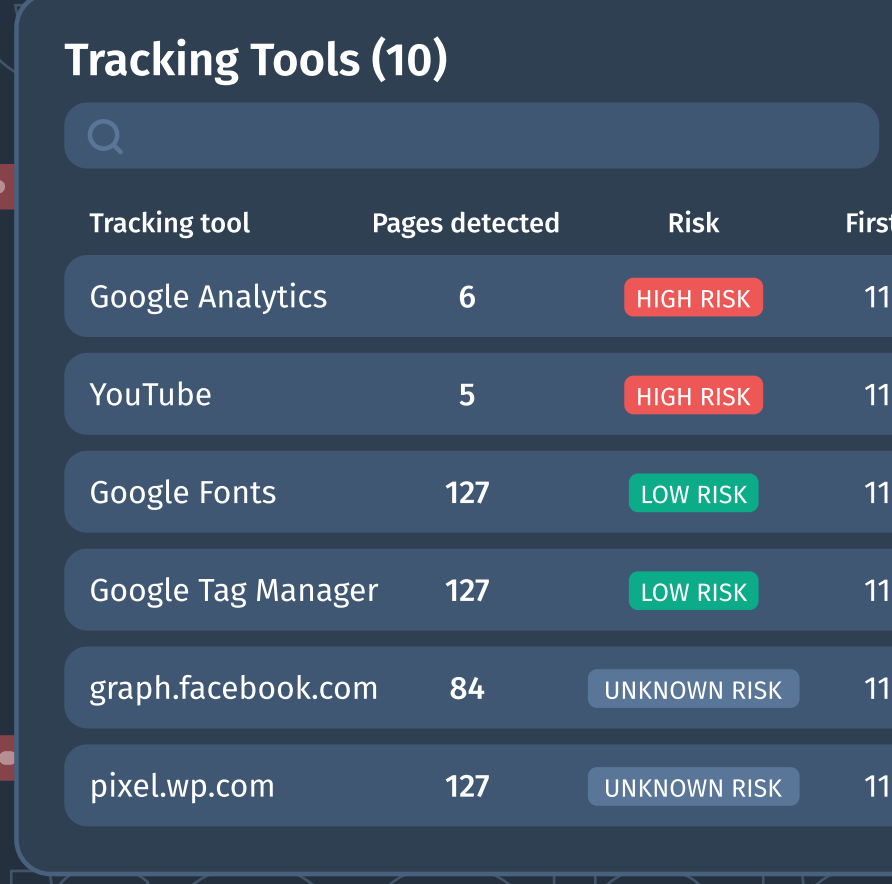
The BAA-protected platform blocks the stream of sensitive data by default and anonymizes each visitor with a unique ID, so you can follow their journey. This means you can remove risky web trackers from your website, but continue using your favorite ads and analytics tools to help you reach your target market.

Check out **WebMD's story** to learn more about how Freshpaint supports privacy-first marketing.

Meet with Freshpaint ↗

About Freshpaint

Freshpaint is a Healthcare Privacy Platform that bridges the gap between patient privacy and digital marketing by ensuring sensitive data is never shared with tools that aren't HIPAA-compliant. Freshpaint replaces untrusted tracking technologies from tools like Google Analytics, Facebook, and Google Ads, then provides a governance layer that controls what data gets shared with those platforms.



Want to keep learning?

Visit Freshpaint.io

Contact us at sales@freshpaint.io

Connect with us on LinkedIn

Meet with us