

What the Recent AHA Lawsuit Ruling Means for Healthcare Organizations Moving Forward



Table of Contents

Before You Read	3
What the Recent AHA Lawsuit Ruling Means for Healthcare Organizations Moving Forward	3
How Did We Get Here	4
What Happened in the Judge's Order?	4
What Happens Next?	5
5 Risks to Keep in Mind Moving Forward	6
HIPAA Is Still A Focus For Healthcare	6
FTC Enforcement	7
State Privacy Laws	8
Class Action Lawsuits	8
Brand Trust	9



Before You Read

Like the AHA ruling, the past two years have seen a whirlwind of lawsuits, court rulings, and new guidance for healthcare organizations. We know it's hard to keep your finger on the pulse 24/7. That's why we created the [Freshpaint Privacy Hub](#): your one-stop shop to stay up-to-date with the ever-evolving world of healthcare privacy.

This is where you can go to escape the clickbait and get down to what matters. Bookmark this page for the latest updates, insights, and resources to keep your organization up to speed.

Healthcare Privacy Hub

Your one-stop shop to stay up-to-date with the ever-evolving world of healthcare privacy.

[Learn More](#) ➔

- reactions
- industry news
- real-time updates
- protected health information
- resources
- marketing performance
- legislation analysis

What the Recent AHA Lawsuit Ruling Means for Healthcare Organizations Moving Forward

At [Freshpaint](#), it's our mission to help healthcare organizations adapt to the ever-evolving world of privacy compliance. The latest development came when a federal court ruled that guidance prohibiting the use of third-party tracking technologies on hospitals' public-facing websites was unlawful.

We've spoken to dozens of healthcare leaders who are curious (rightly so) about how this ruling might impact their marketing strategy. But before we explore what lies ahead, let's rewind to get some context.

How Did We Get Here

In December 2022, HHS updated its HIPAA guidance, making it clear that tracking technologies on healthcare websites could violate federal privacy rules by sharing sensitive consumer health information with third-party tools.

By default, web trackers collect HIPAA identifiers, such as IP addresses, Ad Click IDs, and even email addresses, as well as health information like page URLs and button text. Those two components combined are considered Protected Health Information or PHI—and the HHS concluded that sharing PHI with a non-HIPAA-compliant tool was a privacy violation.

Fast forward to November 2023: The American Hospital Association (AHA) and others filed a federal lawsuit calling on the courts to bar enforcement of OCR’s policy, taking aim at the “Proscribed Combination.” Translation: They argued that an individual’s IP address combined with a visit to a specific web page isn’t sufficient to constitute PHI.

Proscribed Combination = IP Address + Health Information on a publicly facing website

What Happened in the Judge’s Order?

Most recently, on June 20, 2024, US District Judge Mark Pittman sided with AHA, ruling that HHS overstepped in issuing its December 2022 guidance around the Proscribed Combination.

However, he didn’t go any further in his ruling to change any other aspects of the HIPAA guidance. This is a really important distinction because if you’re reading this news thinking that the judge erased the rules around HIPAA on a publicly facing website, that’s not what happened.

This is an important decision but a very narrow one. Let’s explore in detail how healthcare organizations should think about privacy moving forward.

Unlock High Performance Marketing & Protect Patient Privacy

[Learn more ↗](#)

Your Website

Facebook, Google Analytics, Microsoft

What Happens Next?

Judge Pittman vacated the HHS guidance around the combination of users' IP addresses and health information. But he denied the request for a permanent injunction and did nothing to address the combination of other HIPAA identifiers with health information captured by tracking technologies.

Accordingly, many law firms are advising covered entities to continue safeguarding patient privacy, regardless of the recent ruling. According to a number of attorneys we've spoken to, the growing sentiment is that HHS will almost certainly appeal Judge Pittman's decision within the next few days and request a stay. A stay if granted would be likely to occur within days.

Several legal experts shared their opinion with us that in a case like this against the federal government, it's likely that a stay would be granted—especially if it's viewed by the court that the government didn't try to intentionally harm the plaintiff (the AHA and healthcare organizations involved in the lawsuit).

If the stay is granted the HIPAA guidance around IP addresses will be fully restored until the appeal process has run its course.

The first step in the appeals process would move the case to the United States Court of Appeals for the Fifth Circuit. Legal experts we spoke to with experience in federal courts cases told us this could be a 9-12 month process before any judgment gets handed down. If a stay is granted, that means the full HIPAA guidance would be in effect during that period.

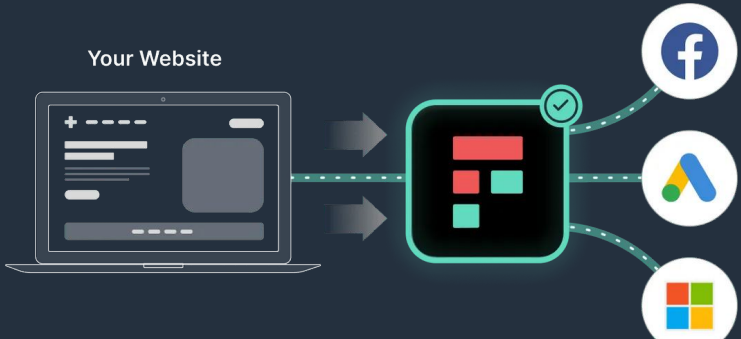
If the appeal is unsuccessful, HHS could take their case to the Supreme Court. If the Supreme Court decided to hear the case, that could add another 12 months to the appeals process. Once again, if a stay was granted, it's likely that the full HIPAA guidance would be in effect for the entire two years of the appeals process.

We certainly don't have a crystal ball to predict how this all will pan out. But it's important to remember that broad, sweeping changes rarely happen overnight. The broader issue of web trackers will continue to be an issue for covered entities, regardless of what comes next in this process.

Unlock High Performance Marketing & Protect Patient Privacy

[Learn more ↗](#)

Your Website



Let's spend a minute discussing the existing risks.

5 Risks to Keep in Mind Moving Forward

Judge Pittman's ruling was an important but narrow one. The order only addressed the prescribed combination of IP addresses on publicly facing healthcare websites and didn't touch any other aspects of the HIPAA guidance. In fact, most of the risks around consumer privacy haven't changed. Here are five to stay aware of.

HIPAA Is Still A Focus For Healthcare

The ruling vacated the small portion of OCR's guidance about collecting a visitor's IP address on a hospital's website. **However, the rest of OCR's tracking tech guidance remains entirely intact.** That means HHS can enforce other instances where HIPAA identifiers are combined with health information—for example, an ad click ID combined with a scheduled doctor appointment shared with an ad platform like Facebook, or a device ID collected by Google Analytics on a condition-specific web page. Almost every healthcare marketing team we've spoken with leverages advertising tools to reach consumers. This is still a major risk for healthcare.

Accordingly, we believe healthcare organizations should continue replacing native tracking technologies with HIPAA-compliant solutions that ensure sensitive health information isn't shared downstream.

But because we aren't healthcare lawyers, we asked one: "What should healthcare organizations do while they await a decision regarding the AHA lawsuit?"



ASK A HEALTHCARE LAWYER

Hear the answer
from a healthcare
legal expert



faegre
drinker

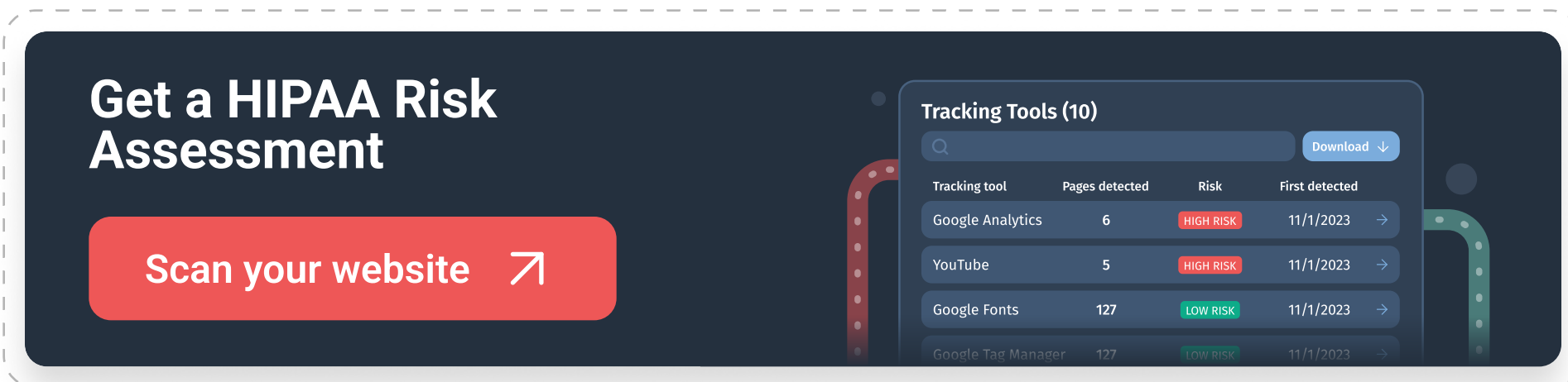


Doriann Cain, a healthcare legal expert and Partner at Faegre Drinker, recommends conducting an analysis to address the complexities and legal challenges associated with tracking technologies, guided by OCR recommendations or other relevant statutes. As a basic compliance measure, it's crucial to understand which tracking technologies are in use and what information they collect, especially in determining what constitutes PHI.

For instance, the presence of dropdown menus, fields for entering personal information, login pages, or search functions for specific providers are key areas to scrutinize, as they might link identifiers with health information.

Clarification is essential, especially if current guidance on the use of tracking technologies on unauthenticated pages is revised. However, the analysis should extend to authenticated pages or those explicitly associated with health information.

Moving forward, organizations should evaluate the risks associated with tracking technologies. While some may choose to disable all tracking to ensure HIPAA compliance, others may prefer to reassess their use of such technologies. It's about balancing the organizational risk tolerance with compliance needs, recognizing that an IP address, in most cases, does not alone constitute PHI.



Tracking tool	Pages detected	Risk	First detected
Google Analytics	6	HIGH RISK	11/1/2023
YouTube	5	HIGH RISK	11/1/2023
Google Fonts	127	LOW RISK	11/1/2023
Google Tag Manager	127	LOW RISK	11/1/2023

FTC Enforcement

The FTC (which operated separately from HHS) regulates for-profit businesses as it relates to consumer privacy. The FTC has a history of enforcing privacy in healthcare. Most recently, [the FTC fined Cerebral \\$7M](#) for disclosing their customers' personal health information to third parties for ads. Further, the FTC banned Cerebral from sharing most data with marketing tools, a catastrophic blow to their customer acquisition strategy.

Even before Cerebral, [the FTC took the same action against BetterHelp](#) in March of 2023 with a fine and ban from using major advertising platforms. More than a year later, BetterHelp is still locked out from critical advertising strategies and instead [spends more on podcast advertising than Google and Amazon combined](#). This is a major blow to a provider that relies on digital advertising channels to reach consumers.

State Privacy Laws

Nineteen states have passed consumer privacy laws—some of them more strict than the HHS guidance issued in 2022. The California Privacy Protection Agency (CPPA) is leading the charge and has [spent the last year preparing to enforce its law](#).

PHI collected for treatment, payment, or healthcare will qualify for the CCPA HIPAA exemption. However, health information collected for other purposes is not covered by the exemption and will be subject to the CCPA's stricter data protection laws.

CCPA defines personal information as anything that could identify, relate, describe, or associate with a specific consumer or household. And the way many state laws are written protects consumers in those states even if the healthcare organization isn't based in that state. So if you provide services to consumers in say California or Washington you could be subjected to those specific state privacy laws.

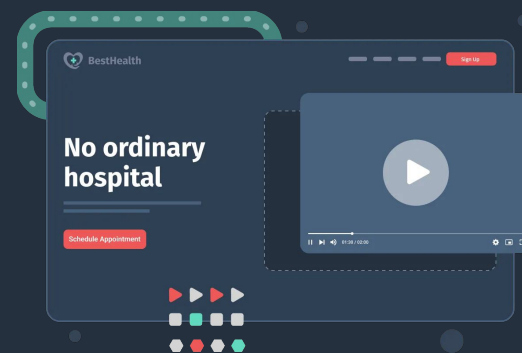
Class Action Lawsuits

Over the past few years, there's been a long list of class action lawsuits filed against major healthcare providers. Aurora Health [settled for \\$12.5M](#) in a class action lawsuit for sharing sensitive health information with ad platforms. [Cedars-Sinai](#), Ascension, UPMC, and Rush University are all being sued as well over claims they shared patient data with advertising platforms. Notice the trend about class action lawsuits against healthcare organizations related to sharing data with major ad platforms?

The current ruling in the AHA lawsuit does nothing to shield healthcare companies from these class action lawsuits—and the negative press that comes with them. In fact, these class action lawsuits typically rely on wiretapping laws and the Video Privacy Protection Act—not HIPAA.

Privacy Related Class Action Lawsuit In Healthcare: How They Work And How To Avoid Them

[Learn more](#) ↗



Doriann [doesn't don't see any change to the risk of class action lawsuits](#) when it comes to the recent IP address change with HIPAA. The absence of a private right of action under HIPAA means plaintiffs turn to the Video Privacy Protection Act and various federal and state wiretapping laws to file suits.

This situation underscores the importance for organizations to thoroughly understand their legal risks and obligations under these statutes. Despite the potential repeal of this guidance, it's crucial for organizations to ensure their privacy policies clearly articulate the use of tracking technologies and comply with the Video Privacy Protection Act and wiretapping laws by obtaining consent before sharing personal information.



Brand Trust

The sentiment amongst consumers is clear: People don't want to be tracked by ad tech companies, especially when their health information is part of the equation. In fact, online privacy protection is a national trend that's nearly universal with consumers.

For healthcare brands it becomes an important question: do you want to be known as a brand that does the minimum when it comes to privacy standards or do the most for your patients?

For healthcare brands it becomes an important question: do you want to be known as a brand that does the minimum when it comes to privacy standards or do the most for your patients?

The AHA's lawsuit has given marketers, lawyers, regulators, and consumers plenty to unpack over the past few days. But we're looking for the signal in the noise—and that signal is that healthcare organizations are still on the hook for safeguarding patient privacy across a growing patchwork of federal, state, and private privacy guidelines.

About Freshpaint

For healthcare brands it becomes an important question: do you want to be known as a brand that does the minimum when it comes to privacy standards or do the most for your patients?

Want to keep learning?

Visit [Freshpaint.io](https://freshpaint.io) ↗

Contact us at sales@freshpaint.io ↗

Connect with us on [LinkedIn](#) ↗

Meet with us ↗

Freshpaint