Freshpaint

ASK A HEALTHCARE LAWYER:

Navigating HIPAA Compliance for Payer Marketing

Table of Contents

Introduction

Since HHS first issued **its guidance** on the use of online tracking technologies, along with **later updates**, health insurers have faced uncertainty. Marketers, compliance, and legal teams within health insurance companies often find themselves without clear directives.

To address this ambiguity, we sought insights from an expert in the field. **Doriann Cain**, a Partner at Faegre Drinker, generously dedicated her time to respond to a wide range of questions.

Read on to get all her answers, or click any of the video thumbnails to hear them for yourself.

P.S. If you want to chat directly with Dori about any of her answers, **fill out this form** and we'll connect you.

What is PHI?

In Dori's interpretation, she explains that PHI is any individually identifiable information about a person's past, present, or future physical or mental health condition, provision of healthcare, or past, present, or future payment of health care.
So here, you're really looking at whether it relates to a physical or mental health condition, the provision of healthcare, or the payment of healthcare. That's what constitutes PHI under HIPAA.

What is health context?

As Dori explains, when thinking about health context from a tracking technology standpoint, you're thinking about what an individual is trying to do on that website.

And by tracking them, can you tell that they're actually trying to obtain some type of healthcare or the provision of healthcare? Are they trying to pay for their healthcare? Or are they trying to address the past, present, or future health condition that they may have?

What is a HIPAA identifier?

In Dori's view, it's helpful to look at this in reverse. OCR has issued guidance regarding the de-identification of PHI. Under that de-identification guidance, OCR states that you have to de-identify 18 different data points for information to actually be de-identified.

So, looking at that in the reverse, OCR states that if those identifiers are tied to a past, present, or future health condition, the provision of healthcare, or the payment of healthcare, that is going to be PHI. So, HIPAA identifiers under that guidance include things like name, address, birthday, social security number, and IP address.

Who is responsible for preventing PHI from being sent to a vendor that isn't a HIPAA business associate?

Dori explains that responsibility sits with the covered entity. They need to be aware of who's a business associate.

Business associates are also directly liable under HIPAA. However, in this instance, if an ad platform specifically states, " We don't want PHI and we're not HIPAA compliant," then that obligation is with the covered entity. So, the knowledge regarding what is and what is not PHI sits with the covered entity. The covered entity should conduct its due diligence to understand what exactly is in that transmission of data.

Who is responsible for ensuring PHI is not sent to a non-covered entity?

Dori explains that responsibility sits with the covered entity. They need to be aware of who's a business associate.

Business associates are also directly liable under HIPAA. However, in this instance, if an ad platform specifically states, " We don't want PHI and we're not HIPAA compliant," then that obligation is with the covered entity. So, the knowledge regarding what is and what is not PHI sits with the covered entity. The covered entity should conduct its due diligence to understand what exactly is in that transmission of data.

Who bears the liability for data collection when a health insurer bids on keywords?

In Dori's view, the liability doesn't sit with the healthcare organization when that ad platform is collecting the data because that is not being done on the healthcare organization's website. There's no tie to that specific covered entity here.

It's essentially an all inclusive type of search where the searcher could go to any healthcare organization that may be connected to those keywords. The information is not stemming from the covered entity.

Is an ad platform considered a business associate if they do not receive PHI?

In Dori's interpretation, yes, that would be acceptable because you're looking at that definition of a business associate. So would that platform be receiving, creating, or transmitting PHI?
And in that instance, if you don't have PHI, you don't have a business associate.

Is an ad click ID considered PHI?

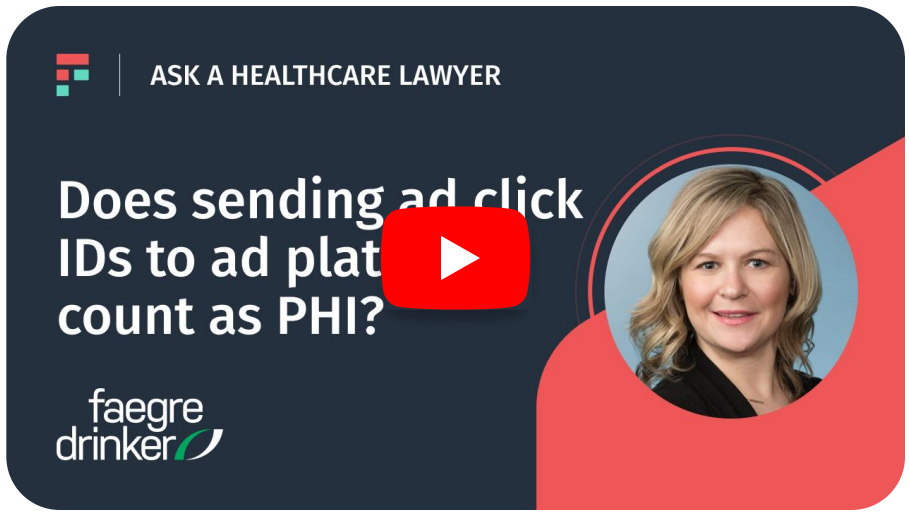
Dori says that an Ad Click ID is very similar to an IP address. So it uniquely identifies an individual.

However, Ad Click ID is not connected to any healthcare information or the payment of healthcare services. It would not constitute PHI. So you have to have that combination, the identification, and then does it relate back to the provision of healthcare services or the payment of healthcare services?

If a health insurer sends an ad click ID back to an ad platform, is that considered PHI?

In Dori's view, this is not PHI under HIPAA because you're not connecting that to the provision or payment of healthcare services.

So, here, you don't have that second component of the definition of PHI. Since you're missing half of the definition, it wouldn't constitute PHI.



If you send two identifiers back to an ad platform, would that be considered PHI?

Dori states that you need to have those identifiers be associated with health information.
And in that context, if you're not connecting that to the provision or payment of health care, then it does not constitute PHI under HIPAA.

Is IP address considered PHI?

According to Dori, the guidance actually created confusion around this. It's clear that tracking technologies on a healthcare entity's authenticated pages collect IP addresses and have access to health context. So in that instance IP addresses get categorized as a part of PHI. But on unauthenticated pages, it's not as clear.

For instance, if a user searches for healthcare services for specific conditions without logging in, the data collected could be considered PHI. This is because the tracking could reveal that the user is seeking healthcare, making even unauthenticated page interactions potentially sensitive.

However, OCR clarifies that not all data collected on unauthenticated pages constitutes PHI, emphasizing that general browsing without a direct healthcare service inquiry typically does not involve PHI collection.

The guidance provides examples of scenarios where unauthenticated page activities, like searching for a doctor for specific symptoms or indicating patient status through a menu, could indeed involve PHI. The key takeaway from the OCR's guidance is that while most unauthenticated page interactions do not constitute PHI, exceptions exist, especially when the user's actions directly relate to seeking healthcare services.

If a consumer is visiting a healthcare insurer's website and not looking for health services, or paying for health services, is their data considered PHI?

Dori clarifies that merely having an identifier on an unauthenticated webpage, where a viewer seeks general information about a healthcare system's foundation, does not constitute Protected Health Information (PHI). If the interaction is limited to gathering information about the foundation without any connection to seeking healthcare services, then, in her interpretation, it does not involve PHI.

Is visiting a healthcare web page considered PHI?

As Dori explains, a visit to a healthcare organization's website does not constitute PHI. There are many different situations in which an individual might visit a website. And so assuming that just viewing a web page is PHI goes above and beyond what OCR would consider PHI.

What other web trackers should health insurers know about besides ad platform trackers?

In Dori's view, there are other web trackers for organizations to monitor. A major thing organizations could really incorporate into their annual risk assessment is obtaining exactly what tracking technologies they're utilizing and what information they're disclosing to those third parties.

This is a project where you look at tracking technologies as a whole and figure out again whether that tracking technology is first-party or third-party.

And then, if it's 3rd party, what information are we disclosing back to that tracking technology, and if anything, does it constitute PHI? And if it does constitute PHI do we have a business associate agreement in place with that organization?

If a healthcare organization only treats one specific condition, would a visit to their homepage constitute PHI?

Dori explains if a healthcare organization specializes in treating a specific condition, visiting its homepage might imply that the visitor intends to receive those services. However, this assumption stretches beyond OCR's intention with its guidance and the definition of PHI.

While initially, one might assume that a page visit directly correlates with seeking healthcare, various reasons, such as inquiries by family members or legal representatives, complicate this assumption. In Dori's view, this interpretation exceeds the scope of what the OCR aims to address in its guidance.
Instead, healthcare organizations should focus on more definitive indicators of intent to receive services, such as the presence of dropdown menus or fields where personal information and intent can be explicitly provided. These elements are more indicative of an individual's attempt to access specific services from the organization.

What is the basis for the AHA lawsuit that came out against the OCR guidance?

Dori explains in November 2023, AHA came out and alleged that the OCR guidance did a few things. One point that they made is that it exceeded OCR statutory authority and violated the Administrative Procedure Act (APA).

Essentially, they view this guidance to be arbitrary and capricious because it did not undergo the proper notice and comment rulemaking process.

Before something can become legally effective, there has to be notice, and individuals get to comment on that. Then, they process those comments, and then something becomes law.

And so their argument is, "Organizations never had an opportunity to respond to this. And so you're violating the APA here."

What should healthcare insurers do while they await a decision regarding the AHA lawsuit?

Dori 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

If AHA wins the lawsuit and the guidance is repealed, will that stop class action lawsuits?

In Dori's opinion, even if the AHA wins its lawsuit against the OCR, it won't halt class action lawsuits. 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.

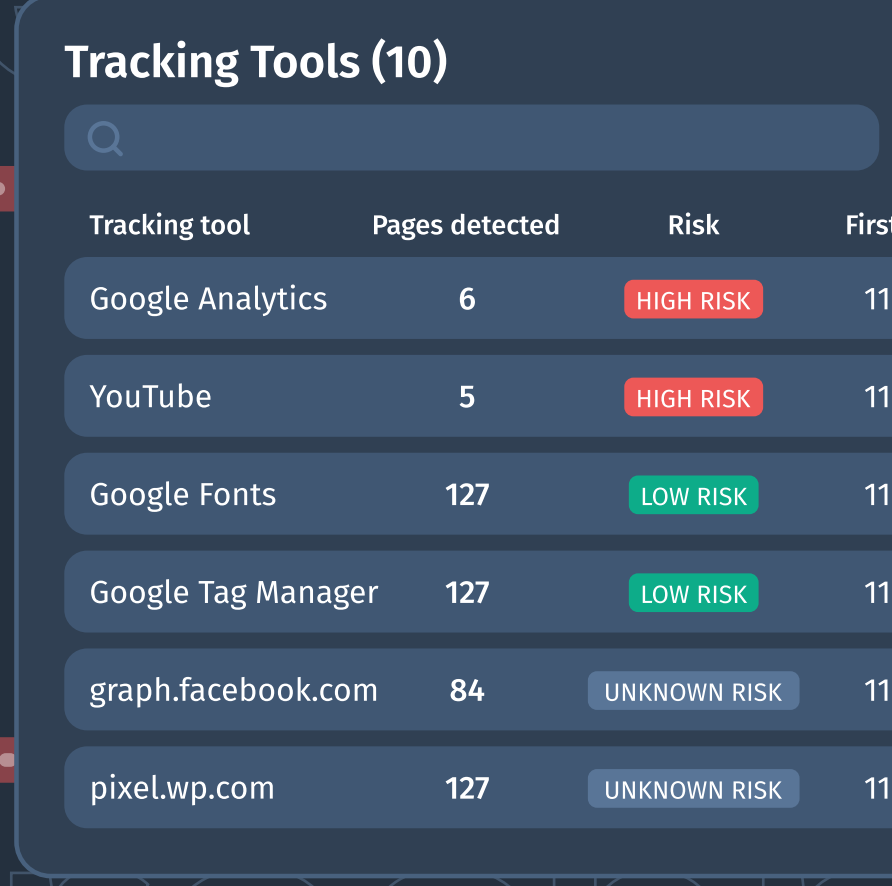
Does HHS want health organizations, including insurers, to stop using ad platforms?

Dori does not believe that HHS's guidance was intended to get healthcare organizations to stop using ad platforms. Instead, she interprets it as a request for them to carefully assess and recognize what constitutes PHI when using ad platforms.

This means healthcare organizations need to be aware of the information they disclose, determine if it qualifies as PHI, and ensure they are entering into BAAs or obtaining authorizations from individuals before any disclosure occurs. It's not about ceasing the use of ad platforms altogether, but about ensuring their use complies with HIPAA standards.

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

Freshpaint