eHealthcare
STRATEGY & TRENDS

HIPAA Compliance 2023: A Guide to Google, Meta, and Other Online Tracking Tools

April 5, 2023

// By James A. Gardner //

In December 2022, the Office of Civil Rights put the hammer down, shoring u HIPAA regulations to cover online tracking technologies that could comprom consumer privacy. Healthcare marketers must take a proactive role in respo

Healthcare marketing is full of important acronyms, but HIPAA (https://ehealthcarestrategy.com/tag/hipaa/) — the federal Health Insura Portability and Accountability Act of 1996 — truly stands alone. Confusin

vague, often misunderstood, and yet backed by stiff penalties, overlooking the HIPAA rules for protecting personal health information is done at your peril.

Like me, you were probably surprised early last summer when The Markup and STAT+ assesse websites of 100 prominent hospitals. On a third of them, they found user tracking technology (https://ehealthcarestrategy.com/tag/online-tracking-technologies/) from Meta — the parent company of Facebook — that was apparently capturing data about pages visited, searches conducted, appointment scheduling, and so forth. Seven of the health systems had installed M Pixel code in their patient portals, exposing Protected Health Information (PHI) (https://ehealthcarestrategy.com/tag/protected-health-information-phi/).

The combination of health information being shared non-consensually with a third party along uniquely identifiable information (https://ehealthcarestrategy.com/tag/personally-identifiable-information/) like an IP address alarmed many. It raised the possibility of, say, a sensitive sear mental health condition or emerging cancer becoming known to Meta and its advertising algo

"It is quite likely a HIPAA violation," noted David Holtzman, a health privacy consultant who previously served as a senior adviser in the U.S. Department of Health and Human Services' O for Civil Rights (OCR), which enforces HIPAA.

OCR then further upped the ante for healthcare marketers in December when it released imp new guidance on all online tracking technologies.

Some form of tracking is essential for marketers. What is a reasonable response to the risks? Concern, not alarm, should be your tone when engaging your organization's leadership. Read learn the six immediate actions you should take to get in front of this, and some possible alter to Google and Meta tracking tools.

OCR's bulletin, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html), emphasizes, "*While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*"

The bulletin continues, "*All such information collected on a healthcare provider's website or mobil generally is PHI, even if the individual does not have an existing relationship with the regulated enti even if the data collected, such as IP address or geographic location, does not include specific treat billing information like dates and types of healthcare services.*"

The message is clear: All our old compliance assumptions about online tracking tools — every from Google and Meta to HotJar and Microsoft — need to be revisited. Ignore the new guidan risk an enforcement action or civil lawsuit. Many of us began to worry.

For a not-eager-to-get-into-trouble healthcare marketer — that's everyone, I hope! — what's a reasonable approach to all this?

First and most important, **engage your marketing, legal, privacy, and/or compliance leade** if you haven't already. They may choose to consult a trained HIPAA attorney. Don't know the ri resource? Contact me for a trusted recommendation.

In tandem, here are six immediate actions you can take:

1. **Get smart on tracking tools and OCR's thinking.** You'll be expected to understand t and help lead your team's thinking. What exactly are tracking tools? Why do we use th What's OCR's concern here?
2. **Remove unused and forgotten tools.** Audit your websites and apps (https://ehealthcarestrategy.com/tag/apps/) regularly to understand the tracking technologies you currently use. Document them and remove any you don't recognize longer use.
3. **Understand what your tools share.** Ignorance is not an excuse; you are responsible knowing where your tools are deployed, what data is collected, where the data is bein transmitted, and limits on use of that data. You may need to consider filing a breach notification (https://ehealthcarestrategy.com/tag/data-breach/) if you've inadvertently noncompliant.
4. **Make a case for your essential tools.** Ensure trade-offs are understood as tools are eliminated from your toolkit. Some tools are critical for successful online marketing, a needs to be made clear. Expect to be asked what other organizations do.
5. **Pursue HIPAA compliance where possible.** Some partners — not Meta or Google, unfortunately — will help your efforts to become HIPAA compliant by signing a Busine

Associate Agreement (https://www.hhs.gov/hipaa/for-professionals/covered-entities/s
business-associate-agreement-provisions/index.html) (BAA).

6. **Scrutinize all future tracking technologies**. Going forward, review all technologies f
third parties with your privacy and compliance teams. No tools should be deployed wi
an assessment of their value and risk.

Where might this all shake out in 2023 and beyond?

There are many types of tracking tools, but those from Google Analytics (https://ehealthcarestrategy.com/tag/google-analytics/) and Meta (https://ehealthcarestrategy.com/tag/meta/) are causing the most angst among healthcare marketers. They're ubiquitously deployed and are close to essential to many marketing teams

I believe we'll see a range of decisions.

Many organizations have already pulled back on Google Analytics, Meta, and all but the most l
technologies while the dust settles. More than a few already operate their websites and apps
analytics or measurement tools at all.

Other organizations may have found a different balance.

Some have configured Google Analytics to anonymize IP addresses before they're stored, an
approach OCR discourages in its guidance. A breach can occur based only on the fact that dat
transmitted to a third party, even if not viewed or used.

Others are exploring the next-gen Google Analytics 4 (GA4) (https://ehealthcarestrategy.com/tag/google-analytics-4-ga4/) platform, which claims to not lo
store IP addresses (https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631) at all. But there are concerns here, too. Other identifiable informati
being collected and even the transmission of data can be problematic, skeptics point out. Goo
(and Meta, for that matter) make no claims of being HIPAA compliant (https://support.google.com/analytics/answer/13297105?hl=en&ref_topic=2919631) and are n
known to sign BAAs.

There's also a solution from Freshpaint (https://www.freshpaint.io/) that claims to scrub all personally identifiable information *before* it gets shared with Google and Meta. Its promises ar interesting, but I'm not quite ready to endorse them.

Self-hosted alternatives to Google Analytics like Matomo (https://matomo.org/) and Piwik Pro (https://piwik.pro/) are also attracting attention. They keep you in control of your data by neve having it leave your possession. But they also come with pros and cons that you should invest

And, of course, some organizations will do nothing. That's highly concerning to me.

Surveying the landscape, Elizabeth Litten, Esq., chief privacy & HIPAA compliance officer at the respected Fox Rothschild (https://www.foxrothschild.com/) law firm, has a similar take.

"OCR's new guidelines are helpful, but they also raise many interesting questions. They'll be addressed over time, but I'm recommending a conservative approach for most organizations until we know more," she told me. "I appreciate that these online tracking tools have business value, but the risk of an expensive and time-consuming enforcement action or civil lawsuit needs to be considered, too. Proceed with caution, I say."

Elizabeth Litten, Esq privacy & HIPAA comp officer at Fox Roths

I hope this article serves as a high-priority call to action for my fellow healthcare marketers.

In the best of times, HIPAA compliance is a complicated and high-stakes challenge. OCR's new privacy guidance is a clear sign that they'll be watching online tracking technologies with a heightened interest. Enforcement actions and civil lawsuits with serious consequences could come unexp to the careless or unprepared.

I encourage you to move quickly, smartly, and with caution.

This article and the links provided are for informational use only and should not be con as legal advice. Contact a qualified attorney to obtain advice specific to your situation.