WebMD Ignite™

WHITE PAPER

How healthcare organizations are approaching the pixel privacy conundrum

Table of contents

Introduction 3

Overview 4

Shifting focus to tracking technology 6

Finding your approach:
Considerations for healthcare organizations 9

Checklist: How partners can help 10

Conclusion 11

Introduction

When the Health Insurance Portability and Accountability Act (HIPAA) became federal law in 1996, the dot-com boom had begun, and the Internet was a skeleton of its current self. Websites and email were in their infancy. But social media? Smartphones? Those were still to come. The notion of scheduling a doctor's appointment or accessing your health records from a computer in your home—let alone from an app on your phone—was beyond popular imagination.

HIPAA was created to protect sensitive patient information within the four walls of a hospital, insurance provider, physician's office, or other physical space of a HIPAA-covered entity. Today, in order to support complex clinical care and a modern patient experience, healthcare organizations have to be able to house and share protected health information (PHI) digitally. Our consumers increasingly expect to find information, schedule appointments, and access their own PHI when, where, and how they want. They expect the same personalized experience from their health providers as they have become accustomed to in almost every other aspect of their lives.

To help provide this seamless, personalized experience, many covered entities' websites and apps contain tracking and measurement tools. These tools provide invaluable insights into consumer behavior. An organization can present tailored messaging that's directly relevant to specific individuals, ultimately helping them to better manage their health by providing the most impactful information in the moments that matter.

HIPAA's guidance on navigating the ever-changing digital landscape hasn't always been timely or even comprehensive. But a Bulletin issued by the Department of Health & Human Services in December 2022 attempted to provide more clarity about how covered entities could use tracking technology while protecting electronic protected healthcare information (ePHI). As a result, covered entities and their business associates must review, refine, and possibly retool (or even retire) some of the technology they have come to rely on to remain HIPAA-compliant.

Overview

In late 2022, the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) issued a Bulletin regarding the obligations of covered entities and their business associates in regards to digital technology and online tracking tools.[1] OCR is responsible for investigating reports of breaches of PHI and noncompliance with HIPAA, which can result in fines for a covered entity or business associate.

A flurry of class-action suits and media coverage about improper tracking usage followed the release of this Bulletin. Many of the lawsuits and much of the press coverage centered around the utilization of Meta's Pixel tracking software—used by many of the top U.S. hospitals and health systems—and other tracking codes.[2]

Although the coverage has been largely negative, the Bulletin spotlighted the potential gaps in securing ePHI and helped to clarify HIPAA rules in regards to websites, apps, and other digital platforms. And it also created the impetus for regulated entities and their business associates to find innovative solutions that balance the need to keep information secure—with the ability to provide a good experience for consumers and patients—and to grow their business.

2022 Bulletin takeaway:

"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. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."

Key moments in history

1996
HIPAA becomes federal law during the Clinton Administration. Websites and email existed but were not close to being as ubiquitous or sophisticated as they are now—and covered entities under HIPAA weren't using them for PHI.

1999
The first marketing-automation platform, Eloqua, is released.

2004
Mark Zuckerberg creates The Facebook with friends at Harvard. Today, the social network has nearly three billion active monthly users worldwide.[3]

2005
Google acquires user-experience and tracking software Urchin and relaunches it as Google Analytics.[4] It marked the start of web tracking as we now know it, signaling a major shift in the digital landscape. Nevertheless, HIPAA guidance failed to address this developing technology.

2009
The Federal Trade Commission issues HIPAA's Final Breach Notification Rule—the first major addition to the regulation. But it still doesn't provide much information about the use of the Internet and other digital technology or tracking modes (like pixels and cookies), or best practices for preventing electronic breaches.

2013
The HIPAA Omnibus Rule is released, which includes discussions of business associates and business associate agreements (BAA). The rule lacks clear guidance on expectations and requirements of digital business associates.

2021
Facebook's parent company, which also includes Instagram, WhatsApp, and Pixel, becomes Meta.

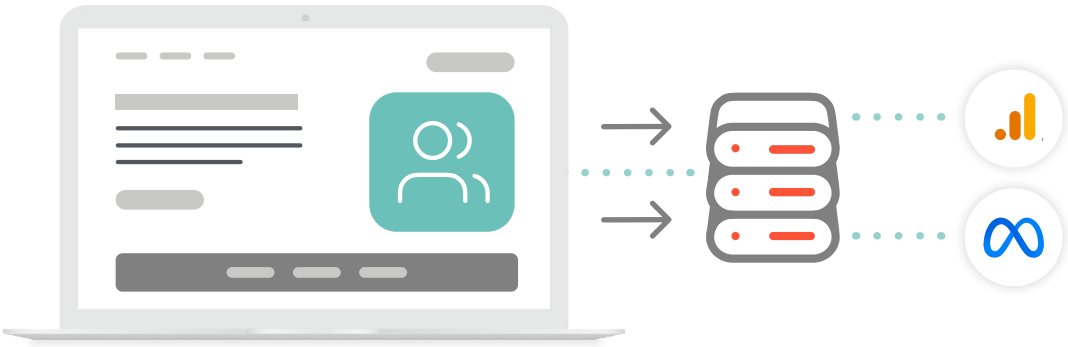
December 2022
OCR and HHS release the Online Tracking Bulletin. This is the first clarification of when tracking codes may be used and when they may be violating HIPAA.

Shifting focus on tracking technologies—and what this means to you

Understanding tracking technology

HHS defined tracking technology in its December 2022 Bulletin as "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." Essentially, a pixel is a snippet of code that tracks users as they navigate through a website, logging which pages they visit, which buttons they click, and certain information they enter into forms. This can then be combined with other information, including an individual's IP address (essentially the unique digital identifier for each internet-connected device) to identify an individual or household.

The information is typically analyzed by a third-party analytics platform, such as Google Analytics. These tools create insights about consumer behavior and experience, both in care settings and on digital properties.



One of the most commonly used tracking codes is the Meta Pixel (formerly Facebook Pixel), which catalogs visitor actions on websites and can be used to create targeted marketing campaigns and enhance conversion tactics. In exchange for installing its pixel, Meta provides website owners with analytics about the ads they've placed on Facebook and Facebook properties and tools to target individuals who have visited their site. In addition, if a patient is logged into Facebook when they visit a hospital's website where a Meta Pixel is installed, some browsers will attach third-party cookies—another tracking mechanism—that allow Meta to link pixel data to specific Facebook accounts.

Here's what HIPAA requires

Websites

Certainly health records accessible online or via an app are considered PHI. All individually identifiable health information (IIHI) provided to a covered entity's website or app that could identify a user and indicates a relationship between the user and entity is PHI and must be treated as such. This information includes their home, email, and IP addresses, as well as dates of appointments and medical device IDs.

When a website is user-authenticated (meaning it requires a unique login and password to access), it usually requires that security layer because it contains PHI. But unauthenticated websites or web pages—such as ones you browse to look for a new physician or to read informative content about a particular condition or procedure—typically do not have access to PHI (though there may be exceptions).

Mobile apps

For regulated entities and their business associates that have their own mobile apps—such as a health clinic with third-party billing—HIPAA Rules apply to protect the PHI gathered by the app. But HIPAA Rules don't extend to mobile apps developed by non-regulated entities where users willingly download or enter health information (like an app in which users track fertility markers to determine optimal conception times). Still, these apps need to abide by privacy and security rules established by the Federal Trade Commission.

Tracked data can lead to consequences

As the HHS Bulletin detailed, *"Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user's mobile device-related information."*

If tracking information is not secure, it can potentially be accessed and misused for identity theft, stalking, harassment, or discrimination. These bad acts can have life-changing consequences for those affected by a data breach, including financial harm, damage to reputation, threats to physical safety, and mental anguish.

Second, there's the matter of trust and transparency. Tracking technology is not always obvious to digital consumers. Sure, we're familiar with a banner asking us to "accept cookies" on websites, but users may not be aware that cookies aren't the only tracking codes being used. It's also likely they are not totally clear how or by whom the data collected by tracking tech is being used. Throw in some lawsuits and bad press, and consumer distrust and fear only grow.

A 2022 analysis by The Markup found Meta Pixel on appointment-scheduling pages of one-third of the top 100 U.S. hospitals, and even in some of their user-authenticated patient portals.[2] In some cases, the Meta Pixel was capturing visitor searches for doctors' names and specific procedures, as well as IIHI, and sending the data back to Meta. Another analysis by researchers at the University of Pennsylvania found nearly 99% of hospital websites contained at least one third-party data transfer, and more than 94% had at least one third-party cookie installed.[5]

Dozens of class-action lawsuits have been filed following data breaches that accessed millions of patients' PHI mined from hospital websites and shared with Google, Facebook, and third-party vendors.[6] All of this places providers in a very precarious position, as Meta has argued that the responsibility lies with the healthcare provider and its web developer, who ultimately control the website code and determine which information to send to Meta.[7]

With all of this publicity, legal action, and general uncertainty, some hospital legal departments are understandably demanding that — in an abundance of caution — every pixel be removed from every page on every web property. But this sort of knee-jerk response is likely to create barriers in building relationships with patients and supporting them in making informed health decisions. It will also potentially have an impact on Marketing's ability to communicate with and attract the new patients needed to drive growth. How do you attract new consumers and convert new customers without the optimization that is standard fare in every other industry?

It seems like each new day brings a new update, new product, and a new platform — plus steeper learning curves. Valuable 1:1 tools that reliably improved the effectiveness of your campaigns may now need to be removed from your toolkit. You may decide to keep them, but will need to spend more money to make them viable within the new regulatory framework.

It all presents quite the conundrum for marketers:

You are charged with helping your organizations grow to stay viable and relevant in your markets. But you can't use the standard digital marketing tool box because using them could put your patients' private data at risk and your organization in the crosshairs of class-action litigators.

Finding your approach: considerations for healthcare organizations & their partners

It's gut-check time: How can you balance financial pressure with your legal responsibility in a constantly changing tech landscape? How do you decide how much tracking and tagging are enough for customer acquisition and satisfaction without compromising ePHI and putting your business in legal jeopardy?

Ultimately, each entity must find the approach that works best for them. A joint dialogue between legal and marketing teams—informed by organizational and consumer needs, and an individualized risk-reward assessment.

Here are some example models covered entities have already adopted:

Approach #1: Unrestricted tracking

This model takes the view that security matters—but not at the expense of growing the business. It incorporates heavy usage of tracking software, including Meta Pixel. A host of analytics platforms track and measure all manner of web engagement, phone calls, web-form conversions, HRA/profiler options, and more. The amount of consumer data collected allows marketing campaigns to be laser-precise, timely, and relevant.

Approach #2: Balanced tracking

In this approach, the safety of ePHI is important, so the organization develops a clear tracking/tagging strategy to support both security and business growth. It maximizes campaign performance by incorporating many of the tried-and-true tools while eliminating others (like Meta Pixel). The organization invests in tech that overlays existing tracking to protect where information goes and allows tagging to manage what data goes to which vendor.

Approach #3: Conservative tracking

In this model, safety of ePHI matters above all else. The organization actively seeks to minimize all risk and exposure to HIPAA violations, regardless of impact to marketing performance. Tag-detection software eliminates any pixel or other type of tracking. Resulting marketing campaigns are set up with the minimum viable pieces to support downstream reports. Any additional monthly reporting is limited to basic ad metrics, like clicks, cost, and impressions.

Next steps to determine your approach

The right strategic partner can introduce a suite of new technology to ensure you're doing everything you can to keep customer data safe and reduce your legal liability.

Here is a list of steps to consider when planning next steps for your organization:

Regularly review your tech stack.

- Know exactly what data is being collected. Keep a running list of third-party trackers to compare this list with your privacy policy and block data-sharing with unauthorized apps.[8]
- Turn off the "advanced data collection" function.
- Review all tools and tracking codes in play. Audit each one to ensure it's HIPAA-compliant.
- Check each website tag and what data each tag is sending to vendors. Assess the risk each tag poses for your business.
- Determine a consistent tech-review schedule (e.g., monthly, bimonthly, quarterly, etc.). This can also help you stay up to date with technology updates or changes.

Explore your software and service options.

- If your current analytics provider hasn't signed a BAA, ask if they will. If not, it may be time to look for a new partner.
- Determine if a new analytics provider can layer their tech over your organization's current analytics system.
- Ask if you can have a free trial to make sure the platform will fit your business needs before committing.

Communicate with your partners.

- Ask what your partners are doing to ensure data security.
- Make sure they understand your company's stance on the following:
  - *What does data privacy mean to your company?*
  - *What are your tagging policies?*
  - *How does each part of your website or mobile app engage with consumers and stay compliant?*
  - *If they have other non-covered clients that may potentially have access to your data through other verticals, how will your partners communicate to them exactly how, when, why, and where it can be used?*
- Vet any new potential partners thoroughly. Make sure they can be trusted with PHI—and can demonstrate how they'll ensure this. Request they undergo a tech review first to verify their security controls are up to your organization's standards.

Chart a path forward.

- Make sure the major players—legal, compliance, IT, data analysis, plus any relevant partners—are on the same page with a strategy and agree on your tech stack.
- Revisit the strategy as needed to stay current and compliant.

Conclusion

It's a tricky balancing act—and an ongoing commitment—to manage HIPAA regulations and digital privacy expectations alongside the need to convert new customers and make their digital experience easy and intuitive. Every healthcare organization is in the same boat. But you don't have to go it alone. WebMD Ignite has partnered with Freshpaint to launch BrandSafe Analytics.

This cutting-edge software is designed to help healthcare providers. Now you can remove non-compliant tracking technologies to support HIPAA compliance, mask individual user data, control data flows across your entire martech stack, and get on with your all-important marketing efforts.

Learn how BrandSafe Analytics helps healthcare organizations.

Learn how

WebMD Ignite™

From Discovery to Recovery, WebMD Ignite is here to activate health with empowering content, engaging education and marketing, and intelligent, integrated clinical workflow solutions. To learn more about our complete suite of care management and member wellness programs, visit webmdignite.com, email us at igniteinfo@webmd.net, or connect with us:

Sources:

[1] U.S. Department of Health and Human Services. 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

[2] The Markup. Facebook is Receiving Seneitive Medical Information from Hospital Websites. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[3] Statista. Number of monthly active Facebook users worldwide as of 1st quarter 2023. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[4] Crunchbase. The Urchin Software Mafia: Becoming Google Analytics and Where They Are Now. https://about.crunchbase.com/blog/san-diego-tech-company-urchin/

[5] HealthAffairs. Widespread Third-Party Tracking on Hospital Websites Poses Privacy Risks for Patients and Legal Liability for Hospitals. https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2022.01205?journalCode=hlthaff

[6] FIERCE Healthcare. Advocate Aurora, WakeMed get served with class action over Meta's alleged patient data mining. https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook

[7] SC Media. Meta punts pixel tool responsibility, says privacy fault is on providers. https://www.scmagazine.com/news/privacy/meta-health-providers-using-pixel-tool-responsible-for-patient-privacy

[8] BNP Media. Data privacy lawsuits explode in healthcare, tech sectors. https://www.securitymagazine.com/articles/98610-data-privacy-lawsuits-explode-in-healthcare-tech-sectors