Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

What does this mean for your health system?

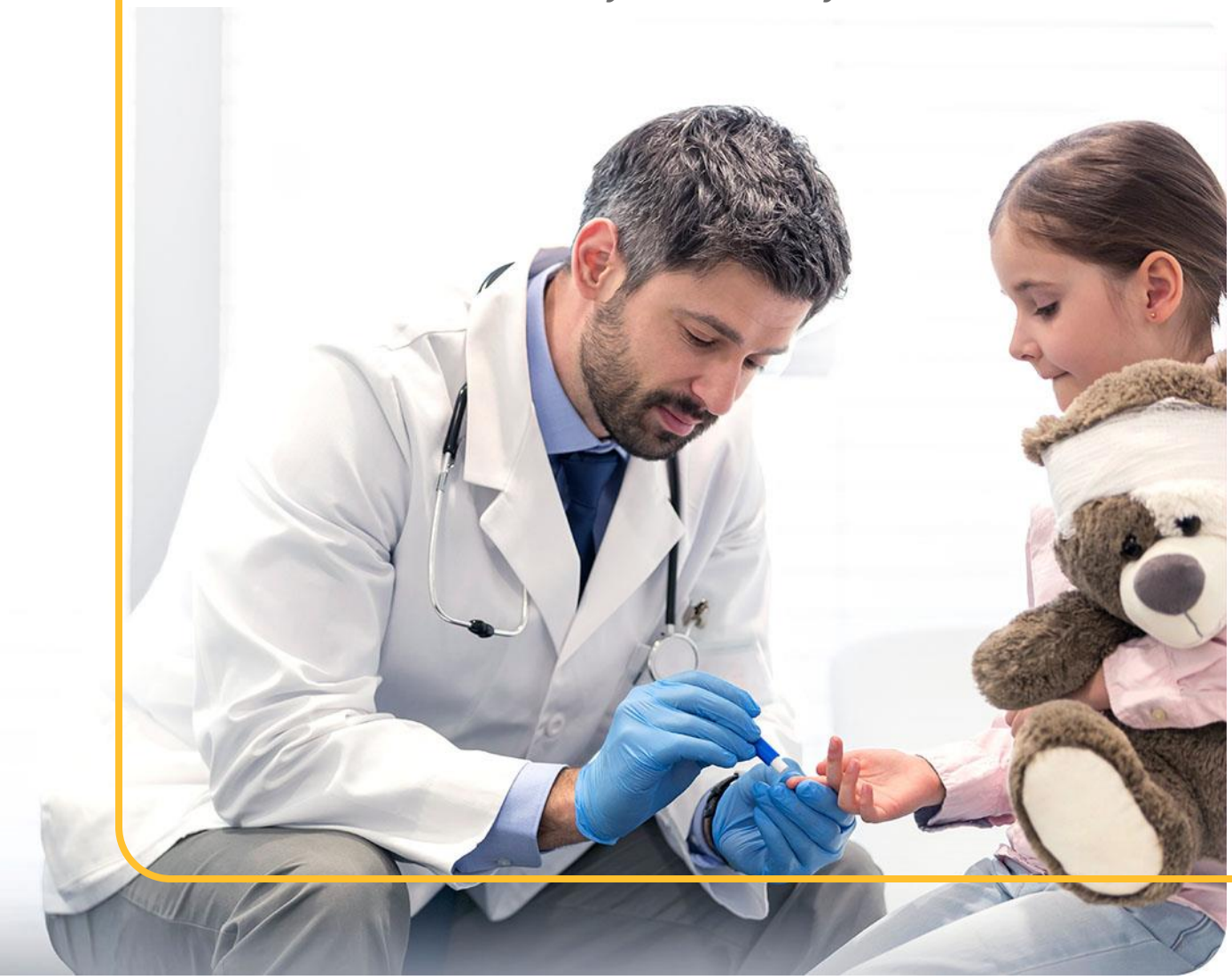

Table of contents

Background & Purpose

On December 1, 2022, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) issued a bulletin titled, “Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates” (OCR Bulletin; 1). The OCR Bulletin highlights the obligations of covered entities and business associates under the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) when using online tracking technologies. In the OCR Bulletin, OCR includes statements on its position regarding: 1) how the HIPAA Rules apply to regulated entities’ use of tracking technologies; and 2) at what point information entered into a provider’s website (either with or without login permissions) becomes subject to the HIPAA Rules.

Over the last several years, there has been a proliferation of consumer online data tracking technologies, which has yielded very valuable information on all consumers visiting websites of all varieties. This valuable information has historically then been used for two key reasons: 1) to help website owners know, understand, and retarget their consumers for enhanced sales; and 2) to be resold to third parties who can then aggregate and analyze consumer information to sell to any number of entities for their various business needs.

When these activities involve Protected Health Information (PHI), the HIPAA Rules are implicated. In addition to potential regulatory enforcement action from OCR, there have been several high-profile legal cases that have demonstrated the risk to providers of the misuse of consumer tracking technologies (e.g., Meta Pixel) in the healthcare marketplace. The consequences of such legal cases can be quite significant, both financially and reputationally.

The OCR Bulletin, coupled with the recent OCR request for more budget and staff to respond to their rapidly increasing backlog of HIPAA enforcement cases (2), may foreshadow a forthcoming era of robust OCR enforcement. Providers should be taking proactive steps to ensure that they understand and comply with the requirements and limitations of the HIPAA Rules with respect to their marketing activities.

The purpose of this white paper is to help Vizient & Sg2 Members understand the application of the OCR Bulletin to their organization, to assess organizational risks that may emerge, and to present considerations for future marketing models that may be required. This document should be used as one of many informational resources consulted by Vizient & Sg2 Members with respect to these topics. This white paper does not provide, and is not a substitute for, legal advice, and we encourage our Members to seek direction from your internal and external counsel for any specific organizational guidance.

Key Points from the OCR Bulletin

The OCR Bulletin focuses primarily on the use of tracking technologies, such as the Meta Pixel, and opens up the aperture for what can now be considered inappropriate PHI data capture, analysis, and usage for the health systems themselves and their web properties.

The following passage from the OCR Guidelines summarizes the primary directive:

> **“The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. 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.”(1)**

While this directive clearly states that tracking technologies cannot be used that would improperly disclose PHI to vendors, the OCR Bulletin expands the scope of what information may constitute PHI to include even the data that an individual searches for and enters on the provider-owned, unauthenticated website. For example, if an individual searches for a pancreatic cancer oncologist on a provider’s site, the OCR Bulletin takes the position that the individual has now disclosed that they likely have pancreatic cancer, and

that information may constitute PHI. This data could potentially be shared/sold with a third party to re-target that person with their businesses' oncology drug regimens for that type of cancer. The OCR Bulletin states:

> **"Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's web page to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply."[(1)]**

This part of the OCR Guidelines was well articulated by a team of legal analysts at 'JDSUPRA.com' as follows:

> **"OCR then explained that HIPAA may apply to authenticated websites (like a patient portal) and some unauthenticated websites because the individual's presence on the website or app is "indicative that the individual has received, or will receive, health care services or benefits from" the entity. In practice, this means that companies subject to HIPAA need to carefully consider how tracking technologies are being used on all of their web pages and apps."[(2)]**

Furthermore, if a provider chooses to purposely collect PHI data and share it with a third-party web-data analysis vendor, such as Google Analytics, it is required that the provider have a fully HIPAA-compliant Business Associate Agreement (BAA) with that vendor, with all of the protections and obligations that entails for both parties, or that the provider obtain a HIPAA-compliant Authorization from the individual before disclosing their data to the vendor. Standard privacy policy acceptance tools on providers' web properties are unlikely to be sufficient to satisfy the stringent requirements of an Authorization. It is also insufficient only to obtain the vendor's promise to remove or de-identify the user's data prior to sending third parties, as the initial disclosure to the vendor must itself be HIPAA compliant.

What providers should do:

The first step is to identify and review any tracking technologies utilized on the provider's websites, appointment forms and/or patient portal. When utilizing technology products for your online entities, it is key to understand which specific technology is being utilized and what information may be transmitted by using it. Commonly used technology products include Meta Pixel, Google Analytics, Google Maps, Yelp, HotJar, Microsoft Clarity, and Crazy Egg, to name a few. If these tools are being used to collect data on a provider's native web properties, then providers should consult advisors immediately to evaluate the need for action, such as disabling those tools. If a provider chooses to still deploy these technologies, then the provider must ensure that they are deployed in a HIPAA-compliant way.

The second step is to review the data collected, analyzed, and transmitted to any third-party platforms that could be deemed PHI. Many third-party marketing vendors engaged with hospitals require this type of data to do their targeting and retargeting of consumers in their markets, so caution is advised. If such data is being collected by, and/or shared with a third-party vendor, assess if the value that the vendor delivers is truly essential for successful provider growth. If so, then move to set up a fully HIPAA compliant BAA and ensure that all safeguards are in place so that no unauthorized PHI disclosures occur. If not, or if a BAA relationship is not an acceptable solution to either party, then consider moving away from that vendor's solution.

Consider a cautious approach. Given the nature of the OCR Bulletin, it is difficult to assess exactly what OCR would deem a breach under the HIPAA Rules until actual legal enforcement actions are taken in the marketplace. Until that time, the path of caution is advisable. To avoid the challenges listed above, providers should consider deploying fully protected and HIPAA-compliant in-house tools to conduct their analytics, thus safeguarding any sensitive information by creating a 1-to-1 data relationship with their consumers.

Here are some tips for providers to help them comply with the position taken in the OCR Bulletin:

- Determine whether tracking technology vendors meet the definition of a business associate and enter a compliant BAA.
- When required, obtain clear and express HIPAA-compliant Authorizations from patients before using online tracking technologies to collect their personal information (e.g., just accepting cookies or an embedded privacy policy may be insufficient).
- Take reasonable steps to protect patient privacy when using online tracking technologies.
- Be transparent about the use of any online tracking technologies.
- Educate patients about their privacy rights.
- Address the use of tracking technologies in the regulated entity's Risk Analysis and Risk Management processes.
- Provide breach notification to affected individuals, the HHS Secretary, and the media (when applicable) of an impermissible disclosure of PHI to a tracking technology vendor.
- Cooperate with OCR investigations.

What providers can still do:

Providers are still fully capable of conducting standard reputational and brand awareness campaigns, such as television ads, social media ads, radio ads, sports/events sponsorships, billboards, etc. Building trust and awareness for a provider's exceptional capabilities, rankings, new service lines, and new sites of care delivery lie comfortably in the purview of the provider's marketing departments.

In terms of direct engagement with consumers in their markets, provider marketing teams can still analyze all the engagement activity with their ads, websites, and portals to understand market demand for services and conditions. Where risk addressed by the OCR Bulletin arises is in the disclosure of PHI to third parties outside the provider's internally HIPAA compliant and protected systems without that third party vendor having proper HIPAA-compliant protections as well.

What the future consumer engagement model looks like:

Providers should look to a future consumer engagement model that is a combination of internally managed brand awareness, internal analysis of direct consumer engagement with ads and hospital web properties, and third party "direct-to-healthcare consumer" platforms and solutions.

By bringing much of what was formally outsourced in-house, provider marketing teams can assert more direct control over all aspects of consumer and patient health data privacy. To this end, providers can increase confidence that they can assure everyone in their markets (and OCR) that their healthcare information is safe, secure, and will not be used by another party in ways that might negatively affect those individuals.

Provider marketing teams should consider engaging with direct-to-consumer third party marketing affiliates that connect directly with healthcare consumers as consumers – not patients – before consumers engage with the provider. By meeting the consumer where they are, helping to educate and motivate the consumers to act for the betterment of their care, and then handing-off those consumers to the provider intake centers, this type of solution avoids the third-party PHI disclosure issues raised by the OCR Bulletin. Such solutions differentiate between who handles consumers as consumers, and who handles patients as patients, facilitating adherence to the attendant data rules that both entail.

Sources

1. 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. What Healthcare Companies Need to Know and Do About Ad Tracking Technologies
https://www.jdsupra.com/legalnews/what-healthcare-companies-need-to-know-6349732/

3. HHS issues guidance on requirements under HIPAA for online tracking technologies, addressing privacy and security concerns related to health information.
https://www.mwe.com/insights/hhs-issues-guidance-on-requirements-under-hipaa-for-online-tracking-technologies-addressing-privacy-and-security-concerns-related-to-health-information/

4. HHS warns HIPAA covered entities and business associates that use of website cookies, pixels, and other tracking technology may violate HIPAA rules.
https://www.healthlawadvisor.com/2022/12/05/hhs-warns-hipaa-covered-entities-and-business-associates-that-use-of-website-cookies-pixels-and-other-tracking-technology-may-violate-hipaa-rules/

5. Is your organization ready for an OCR HIPAA compliance review re: use of online tracking technology?
https://www.legalhie.com/is-ocr-ready-to-review-hipaa-covered-entities-business-associates-for-using-online-tracking-technology/

6. OCR guidance on use of tracking technologies warrants review of website tech.
https://www.bakerdatacounsel.com/information-governance-2/ocr-guidance-on-use-of-tracking-technologies-warrants-review-of-website-tech/

7. FTC to ban BetterHelp from revealing consumers' data, including sensitive mental health information, to Facebook and others for targeted advertising.
https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

8. FTC: STATEMENT OF THE COMMISSION On Breaches by Health Apps and Other Connected devices September 15, 2021.
https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

---

About Vizient, Inc.
Vizient, Inc., the nation's largest health care performance improvement company, serves more than 50% of the nation's acute care providers, which includes 97% of the nation's academic medical centers, and more than 20% of ambulatory care providers. Vizient provides expertise, analytics, and advisory services, as well as a contract portfolio that represents more than $130 billion in annual purchasing volume. Vizient's solutions and services improve the delivery of high-value care by aligning cost, quality and market performance. Headquartered in Irving, Texas, Vizient has offices throughout the United States. Learn more at vizientinc.com.

About Sg2
Sg2, a Vizient company, is the health care industry's premier authority on health care trends, insights, and market analytics. Our analytics and expertise help hospitals and health systems achieve sustainable growth and ensure ongoing market relevance through the development of an effective System of CARE. Learn more at sg2.com

About ShareMD Connect
ShareMD Connect drives rapid impact growth by finding, engaging, and converting qualified, high-lifetime value consumers into your health system. Our mission is to improve the quality of healthcare for everyone by enabling faster service and specialized, human-centric support for more people, not just to the most privileged. Learn more at connect.sharemd.com.

Vizient, Inc.
290 E. John Carpenter Freeway
Irving, TX 75062-5146
(800) 842-5146

ShareMD
10800 Davis Drive
Alpharetta, GA 30009
(832) 937-4273

As the nation's largest member-driven health care performance improvement company, Vizient provides solutions and services that empower health care providers to deliver high-value care by aligning cost, quality, and market performance. With analytics, advisory services, and a robust sourcing portfolio, we help members improve patient outcomes and lower costs.

Sg2, a Vizient company, is the health care industry's premier authority on health care trends, insights, and market analytics. Our analytics and expertise help hospitals and health systems achieve sustainable growth and ensure ongoing market relevance through the development of an effective System of CARE.

To learn more, please contact
Jon Barlow, VP Consumer Innovation
jon.barlow@vizientinc.com.