Barley Snyder

HHS Bulletin Warns Health Care Providers: Make Sure Website Tracking Is HIPAA-Compliant

PUBLISHED ON
December 19, 2022

Earlier this month, the Department of Health and Human Services' Office of Civil Rights issued a bulletin cautioning health care providers that the use of "website tracking" software could be leading to unintended breaches of HIPAA regulations if protected health information is being collected.

Website tracking refers to the now-commonplace practice of website and related mobile application owners collecting detailed data from users, such as all keystrokes and clicks on a page or app. Common tracking tools include cookies, pixels, and mobile software development kits.While this tracking may include helpful internal uses to the owner, such as improving the user experience or finding and correcting bugs, the collected data is also sometimes provided to third parties to drive targeted marketing efforts at users. Website tracking is not without controversy, and the practice has resulted in litigation in Pennsylvania and nationwide, as was discussed in a recent client alert.

HHS took aim at the practice after reports earlier this year highlighted the use of website tracking by healthcare providers, including one report that found some of the largest healthcare systems in the United States were capturing and sending data to Meta (Facebook's owner) through a software program called Pixel when a user scheduled a doctor's appointment online. In its December 1, 2022 bulletin, HHS sought to remind health care providers that website tracking software could be collecting protected health information ("PHI") as defined under HIPAA. If so, providers need to ensure that such data is handled in compliance with the HIPAA regulations, including the Breach, Privacy, and Security Rules.

The bulletin provides several examples of potential PHI that could be collected from a healthcare provider's website or mobile application by tracking software, particularly the authenticated patient portals that many providers use currently. These examples include an individual's IP address, medical record number, home or email addresses, or dates of appointments. The bulletin also cautions that tracking software on a healthcare provider's unauthenticated website - i.e., one that does not need a password to access - could be collecting PHI, such as a patient's login information, a user's search for a health care provider or specialist, or a request to schedule an appointment.

A health care provider should take a multi-faceted approach when it seeks to determine the existence and scope of its PHI collection in compliance with these requirements.For instance, its website management team (i.e., IT, security, and marketing) should understand these requirements, and its compliance team should be educated on the types of technologies its websites and applications may use to collect PHI.If a health care provider is indeed using tracking software and collecting PHI for use internally or providing it to a third-party vendor, HHS warns that the PHI collected needs to be treated in compliance with HIPAA regulations. That means, among other things, that health care providers should:

- Document the actual tracking technology used and what specific data is collected and how it is used and shared;
- Inform users that tracking software is being utilized and that their PHI is being collected;
- Enter into business associate agreements with any third-party vendors who are being provided PHI obtained through tracking software and develop a process to review and document the addition of new vendors who will collect or process PHI. The agreement should reflect the provider's understanding of the tracking technology, what information, if any, is collected, and how it will be used and disclosed;
- Ensure that information collected is not used or disclosed for purposes requiring authorization, such as marketing, in the absence of such authorization;
- Ensure that information collected is not involved in any transactions which could be viewed as the sale of PHI prohibited under the Privacy Rules, Section 164.502(5)(ii);
- Consider the collection, storage, and use of PHI obtained through tracking software when performing a security risk analysis and while implementing the required administrative and technical safeguards to protect PHI; and
- Treat any unauthorized disclosure of PHI obtained through tracking software as a breach under HIPAA, which triggers various reporting and investigation obligations on the part of the health care provider.

While health care providers have long understood that electronic health records, along with their practice management and clinical support software, must comply with HIPAA, this new bulletin makes it clear that additional considerations must be given to its information routinely collected on public-facing websites, applications and other web-based assets.

If you have any questions about how to remain HIPAA-compliant while using website tracking technologies, please reach out to Donald Geiter, Katherine Kravitz, Peter Faben or anyone in the Cybersecurity Service Team.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com

Katherine Betz Kravitz

Partner

Tel: (717) 399-1533

Email: kkravitz@barley.com

Peter J. Faben

Partner

Tel: (717) 208-8844

Email: pfaben@barley.com