Breach Notification , HIPAA/HITECH , Security Operations

Not-So-Cerebral Sharing of Mental Health Data Hits Millions

Website Tracking Tools in Use Since 2019 Exposed Online Mental Health Assessments

Marianne Kolbasuk McGee (HealthInfoSec) • March 10, 2023

Image: Shutterstock

A provider of online mental health services is notifying nearly 3.2 million people that the company used website tracking tools to share sensitive patient information with third parties including Facebook, Google and TikTok - without the individuals' consent.

See Also: OnDemand | Navigating the Difficulties of Patching OT

San Francisco-based Cerebral Inc. in a breach notice says it that recently discovered an issue related to the "inadvertent" sharing of HIPAA-protected health information, including online mental health assessments, through its use of pixels and similar web tracking technologies.

The company on March 1 reported the incident to the Department of Health and Human Services as an "unauthorized access/disclosure" breach affecting 3.17 million individuals. The practice of sharing this information dates back to 2019.

Breach Details

The company says that on Jan. 3 it determined that it had disclosed certain PHI to some third-party platforms and subcontractors without having obtained HIPAA-required assurances.

Since that discovery, the company says, it has disabled, reconfigured or removed the tracking technologies on its platforms and discontinued data sharing with any subcontractors unable to comply with HIPAA requirements.

"In addition, we have enhanced our information security practices and technology-vetting processes to further mitigate the risk of sharing such information in the future," Cerebral says.

Sensitive Data

A wide range of information appears to have been potentially shared through the web tracking tools. Cerebral says information disclosed includes names, phone numbers, email addresses, birthdates, IP addresses, Cerebral client ID numbers and other demographic information.

The firm says it also disclosed online mental health self-assessments, including the service that individuals selected, assessment responses and certain associated health information.

For individuals purchasing a Cerebral subscription plan, the information disclosed may have included the type of subscription plan, appointment dates and other booking information, treatment, clinical information, health insurance and pharmacy benefit information and insurance co-pay amounts.

Social Security numbers, credit card information and bank account information were not among the data shared, Cerebral says.

Concerning Disclosures

Privacy and security attorney Cory Brennan of the law firm Taft says Cerebral's detailed explanation of the information shows the company's investigation into the matter was thorough.

"That being said, the type of information that is particularly concerning in this situation is pretty clear and exactly what we advise clients who are using third-party tracking technologies to be aware of," she says.

"Tracking technologies implemented on any part of a provider website that includes what we typically categorize as 'interactive tools' - such as symptom checkers, health risk assessments, appointment scheduling, account registration and treatment cost estimates - absolutely have the ability to collect and transmit individually identifiable health information," Brennan says.

The nature of interactive tools themselves understandably impacts the sensitivity level of the information transmitted, she says.

"In Cerebral's case, an individual's responses to the mental health self-assessment may be extremely sensitive in nature, and sharing this information with third-party tracking technology vendors like Google, Meta and TikTok creates a significant privacy concern."

Growing Problem

Cerebral is the latest of at least four other entities reporting major health data breaches to HHS OCR in recent months involving their previous use of tracking tools such as Meta Pixel and Google Analytics on health-related websites (see: *Clinic Reports Tracking Pixel Breach Involving 3rd Party*).

Also, the Federal Trade Commission on Feb. 1 announced a $1.5 million civil penalty against GoodRx, saying the telehealth and discount prescription drug company for years shared sensitive personal health information with third-party companies contrary to its privacy promises (see: *FTC Hits Firm With $1.5M Fine in Health Data-Sharing Case*).

Several healthcare organizations that previously used web tracking tools on their website and patient portals, including Cedar Sinai Medical Center in Los Angeles, also face proposed class action lawsuits.

Meta, parent company of social media giant Facebook, is also a defendant in several proposed class action lawsuits in a San Francisco federal court involving the use of the company's Pixel tracking code on healthcare-related websites (see: *Federal Judge Skeptical of Facebook in Patient Privacy Suit*).

Regulatory Warning

HHS OCR issued guidance in December warning that entities covered by HIPAA cannot use the website tracking code if the trackers transmit protected health information without patient consent or if the entities don't have a signed business associate agreement with the technology tracking vendors (see: *HHS: Web Trackers in Patient Portals Violate HIPAA*).

Privacy attorney Mark Swearingen of the law firm Hall Render says he expects to see many more breach reports being filed to regulators as organizations review their use of web tracking technologies on healthcare provider and health plan websites.

"OCR guidance and subsequent comments from OCR officials have made it clear where they stand on this issue, and did not leave much room for alternative interpretations," he says.

"OCR has initiated detailed compliance reviews of several organizations and I think they will continue to take the time to thoroughly investigate these cases before bringing an enforcement action," he adds.

The privacy issues around web tracking have created a very uncertain environment for legal, compliance, IT and marketing departments at health-related organizations throughout the country, Swearingen says. "Any healthcare organization with a website should be carefully reviewing its use of web tracking technologies to be sure that those activities are occurring in a compliant manner."

About the Author

Marianne Kolbasuk McGee

Executive Editor, HealthcareInfoSecurity, ISMG

McGee is executive editor of Information Security Media Group's HealthcareInfoSecurity.com media site. She has about 30 years of IT journalism experience, with a focus on healthcare information technology issues for more than 15 years. Before joining ISMG in 2012, she was a reporter at InformationWeek magazine and news site and played a lead role in the launch of InformationWeek's healthcare IT media site.