MERCOLA
Take Control of Your Health

Does Facebook Have Your Medical Records?

Analysis by Dr. Joseph Mercola ✔ Fact Checked | July 19, 2022

STORY AT-A-GLANCE

- Facebook's Meta Pixel was found on 33 hospital websites, sending Facebook information linked to an IP address, which identifies individual computers and may be traceable back to an individual or household
- The pixel tracks what doctors are searched for and health-related search terms added to search boxes or selected from dropdown menus
- The Meta Pixel was found in patient portals from seven health systems; data being collected included names of medications being taken, descriptions of allergic reactions and upcoming doctors' appointments
- More than 26 million patient admissions and outpatient visits have been shared by the 33 hospitals using Meta Pixels, and that's likely conservative

By now, most people are aware that if they "like" a certain page on Facebook, it gives the social media giant information about them. "Like" a page about a particular disease, for instance, and marketers may begin to target you with related products and services.

Facebook may be collecting sensitive health data in far more insidious ways as well, however, including tracking you when you're on hospital websites and even when you're in a personal, password-protected health information portal like MyChart.[1]

It does this via pixels, which may be installed without your knowledge on websites you visit. They can collect information about you as you browse the web, even if you don't have a Facebook account.

Meta Pixel Found on Hospital Websites

In particular, the Meta Pixel is a piece of JavaScript code that developers can add to their website to track visitor activity.[2] According to Meta:[3]

> *"It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for dynamic ads campaigns, and to analyze that effectiveness of your website's conversion funnels."*

Even hospitals are opting into the data trackers, as evidenced by an investigation by The Markup, which tested websites from Newsweek's top 100 U.S. hospitals. Facebook's Meta Pixel was found on 33 of the websites, sending Facebook information linked to an IP address, which identifies individual computers and may be traceable back to an individual or household.

The pixel tracks not only the IP address of the computer being used but also what doctors are searched for and search terms added to search boxes or selected from dropdown menus. The Markup reported:[4]

> *"On the website of University Hospitals Cleveland Medical Center, for example, clicking the "Schedule Online" button on a doctor's page prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the search term we used to find her: "pregnancy termination."*
>
> *Clicking the "Schedule Online Now" button for a doctor on the website of Froedtert Hospital, in Wisconsin, prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the condition we selected from a dropdown menu: "Alzheimer's.""*

Meta Pixel Installed on Patient Portals

Health care is increasingly going digital, making the privacy of patient portals like MyChart increasingly important. In 2020, about 6 in 10 Americans were offered access to an online patient portal — a 17% increase since 2014 — and close to 40% accessed their records online at least once.[5]

Overall, about one-third of those who used patient portals downloaded their online medical records in 2020, which is nearly double the amount that did so in 2017.

However, the data you're accessing when using password-protected patient portals may also be sent to Facebook via pixels. The Markup found the Meta Pixel in patient portals from seven health systems, including Edward-Elmhurst Health, FastMed, Novant Health and Community Health Network.

Data being collected included names of medications being taken, descriptions of allergic reactions and upcoming doctor's appointments.[6] Novant Health, which removed the pixel after being contacted by The Markup, stated, "We appreciate you reaching out to us and sharing this information. Our Meta pixel placement is guided by a third party vendor and it has been removed while we continue to look into this matter."[7]

The Markup is now collaborating with Mozilla Rally, using a browser add-on and crowd-sourcing to send data about the Meta Pixel on websites visited by study participants. The aim of the study, which runs through July 13, 2022, and has been dubbed the Facebook Pixel Hunt, is to map Facebook's pixel tracking network to better understand the types of information being collected across the web.[8]

'Quite Likely a HIPPA Violation'

The federal Health Insurance Portability and Accountability Act (HIPAA) makes it illegal for hospitals to share personally identifiable health data with Facebook and others, unless an individual has consented to it. As a result, it's possible that Facebook's Meta Pixel on hospital sites is illegal.

David Holtzman, a former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, told The Markup, "I am deeply troubled by what

[the hospitals] are doing with the capture of their data and the sharing of it. I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA violation."[9]

By June 15, 2022, at least seven of the hospitals that The Markup contacted had removed pixels from their appointment booking pages, while at least five of the health systems with Meta Pixels on their patient portals had removed the pixels.

However, to get an idea of the scope of the data being released, The Markup found that more than 26 million patient admissions and outpatient visits had been shared by the 33 hospitals using Meta Pixels, and that's likely conservative.

"Our investigation was limited to just over 100 hospitals; the data sharing likely affects many more patients and institutions than we identified," The Markup reported.[10] In fact, anytime you browse the web you're likely to come across a Meta Pixel, as they're found on more than 30% of the most popular websites online.[11]

IP addresses are listed as one of the identifiers that can make data count as protected health information under HIPPA. Further, being logged into Facebook when visiting a hospital website with a Meta Pixel may allow even more tracking mechanisms, such as third-party cookies, to be attached, so pixel data can be linked to Facebook accounts. According to The Markup:[12]

> *"[I]n several cases we found — using both dummy accounts created by our reporters and data from Mozilla Rally volunteers — that the Meta Pixel made it even easier to identify patients.*
>
> *When The Markup clicked the "Finish Booking" button on a Scripps Memorial Hospital doctor's page, the pixel sent Facebook not just the name of the doctor and her field of medicine but also the first name, last name, email address, phone number, zip code, and city of residence we entered into the booking form."*

Patients Would Be 'Shocked'

It's quite possible that what Facebook is doing with sensitive patient health data is illegal, but even if it's not, most people would be shocked to find out the types of data that Facebook is collecting about them online, when they're using what are assumed to be private, protected health websites and patient portals.

Speaking with The Markup, Glenn Cohen, faculty director of Harvard Law School's Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics, explained:[13]

> *"Almost any patient would be shocked to find out that Facebook is being provided an easy way to associate their prescriptions with their name. Even if perhaps there's something in the legal architecture that permits this to be lawful, it's totally outside the expectations of what patients think the health privacy laws are doing for them."*

While Facebook claims that it uses machine-learning systems to detect sensitive health data and block it from being collected, hundreds of websites from crisis pregnancy centers were found to be sharing visitor information with the social media giant, include information such as whether the visitor was seeking pregnancy tests, emergency contraceptives or abortion.

The data could be used to direct targeted advertisements or even, in a worst-case scenario, potentially in legal proceedings.

Albert Fox Cahn, founder and executive director of the Surveillance Technology Oversight Project, told The Markup, "I think this is going to be a wake-up call for millions of Americans about how much danger this tracking puts them in when laws change and people can weaponize these systems in ways that once seemed impossible."[14]

Google Is Also Tracking Health Data

In 2019, Google partnered with the University of Chicago Medial Center to collect medical records and use artificial intelligence to predict medial events. The records were supposed to be anonymous, but they included date stamps and doctors' notes,

which the lawsuit alleged Google could combine with geolocation data to identify patients.[15]

The lawsuit alleged, "The personal medical information obtained by Google is the most sensitive and intimate information in an individual's life, and its unauthorized disclosure is far more damaging to an individual's privacy" than data typically exposed in hacks, such as credit card numbers.[16]

Four attorneys general have also sued Google for its deceptive practices in collecting location data from the public. The separate lawsuits allege that Google continued to track location data of its users even after they had disabled location tracking.

Karl A. Racine, attorney general for the District of Columbia, initiated an investigation into Google after a 2018 AP News report revealed Google was tracking people's movements even when they'd opted out of such tracking.[17] Google's misleading claims to users regarding privacy protections available in their account settings have been ongoing since at least 2014, Racine's investigation found.[18]

Aside from hiding location tracking under settings users wouldn't expect, like Web & App Activity — which is turned on by default — Google is accused of collecting and storing location information via Google services, Wi-Fi data and marketing partners, again after device or account settings had been changed to stop location tracking.[19]

In addition to the District of Columbia, the attorneys general of Texas, Washington and Indiana have also filed lawsuits against Google for their deceptive data collection practices. The suits allege that Google also pressured users to use location tracking more often because it claimed — falsely — that its products wouldn't function properly without it.[20]

Location data, meanwhile, can be used to reveal intimate details about your life, from your gym memberships, health care visits, stores and restaurants you frequent to where you go to church. It may also be used to provide personalized ads on digital billboards as you pass by, and Google tracks, and provides to its customers, information about how well online ads work to drive people into brick-and-mortar stores.[21]

Protect Your Privacy Online

Once you recognize that you're being tracked online, consciously opting out of it as much as possible is wise. Robert Epstein, Ph.D., a senior research psychologist at the American Institute for Behavioral Research and Technology (AIBRT), reminds people that free services online, such as Facebook and Google, aren't really free, as you pay for them with your freedom.[22] To take back some of your online privacy, for yourself as well as your children, he recommends:[23]

1. Get rid of Gmail. If you have a Gmail account, try a non-Google email service instead such as **ProtonMail**, an encrypted email service based in Switzerland.
2. Uninstall Google Chrome and use **Brave** browser instead, available for all computers and mobile devices. It blocks ads and protects your privacy.
3. Switch search engines. Try Brave search engine instead.
4. Avoid Android. Google phones and phones that use Android track virtually everything you do and do not protect your privacy. It's possible to de-Google your cellphone by getting an Android phone that doesn't have a Google operating system, but you'll need to find a skilled IT person who can reformat your cellphone's hard drive.
5. Avoid Google Home devices. If you have Google Home smart speakers or the Google Assistant smartphone app, there's a chance people are listening to your requests, and even may be listening when you wouldn't expect.
6. Clear cache and cookies. This will help get rid of invasive computer codes that track what you do online.
7. Use a proxy or VPN (Virtual Private Network). This service creates a buffer between you and the internet, "fooling many of the surveillance companies into thinking you're not really you."