GlobalResearch
Center for Research on Globalization

Facebook Is Receiving "Sensitive Medical Information" from Hospital Websites

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

By Todd Feathers, Simon Fondrie-Teitler, and et al.

Global Research, June 18, 2022
The Markup 16 June 2022

Region: USA
Theme: Intelligence

***

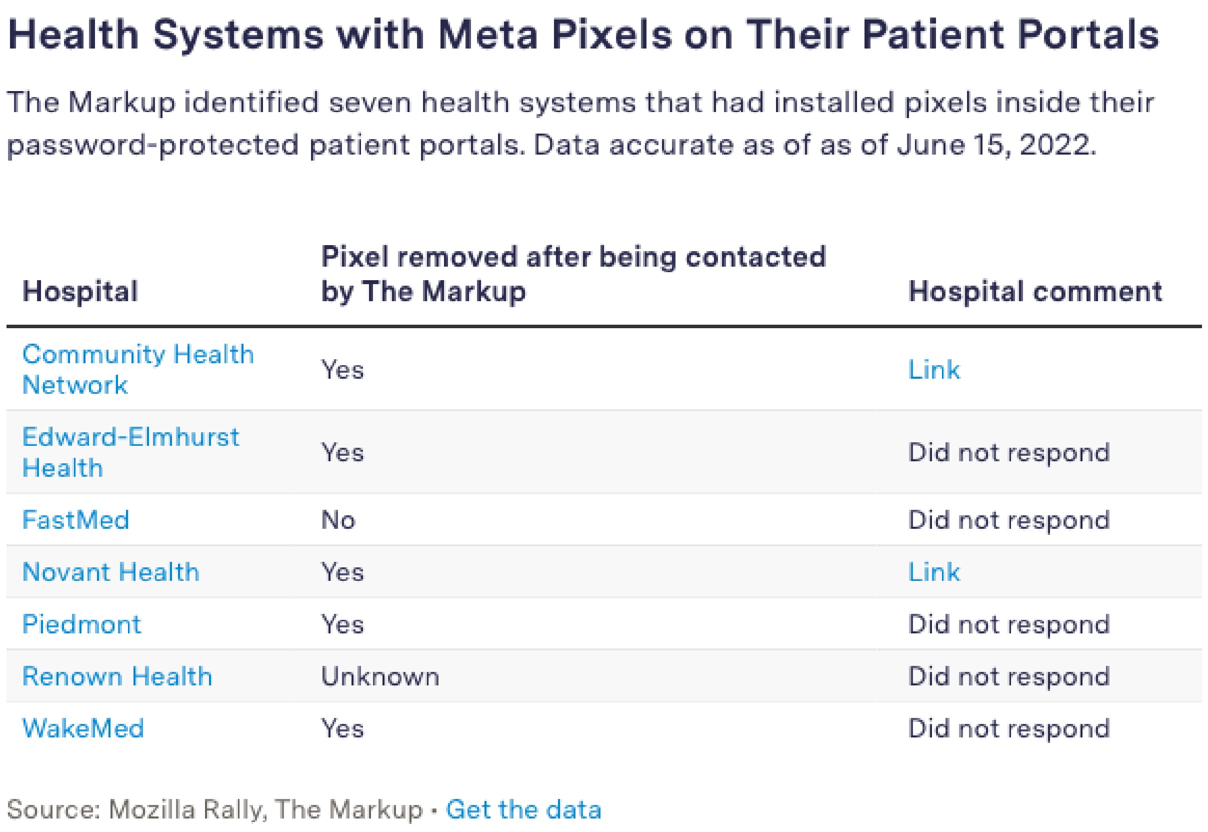
A tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information—including details about their medical conditions, prescriptions, and doctor's appointments—and sending it to Facebook.

The Markup tested the websites of Newsweek's top 100 hospitals in America. On 33 of them we found the tracker, called the Meta Pixel, sending Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. The data is connected to an IP address—an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook.

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."

The Markup also found the Meta Pixel installed inside the password-protected patient portals of seven health systems. On five of those systems' pages, we documented the pixel sending Facebook data about real patients who volunteered to participate in the Pixel Hunt project, a collaboration between The Markup and Mozilla Rally. The project is a crowd-sourced undertaking in which anyone can install Mozilla's Rally browser add-on in order to send The Markup data on the Meta Pixel as it appears on sites that they visit. The data sent to hospitals included the names of patients' medications, descriptions of their allergic reactions, and details about their upcoming doctor's appointments.



Health Systems with Meta Pixels on Their Patient Portals

The Markup identified seven health systems that had installed pixels inside their password-protected patient portals. Data accurate as of as of June 15, 2022.

Hospital	Pixel removed after being contacted by The Markup	Hospital comment
Community Health Network	Yes	Link
Edward-Elmhurst Health	Yes	Did not respond
FastMed	No	Did not respond
Novant Health	Yes	Link
Piedmont	Yes	Did not respond
Renown Health	Unknown	Did not respond
WakeMed	Yes	Did not respond

Source: Mozilla Rally, The Markup • Get the data

Former regulators, health data security experts, and privacy advocates who reviewed The Markup's findings said the hospitals in question may have violated the federal Health Insurance Portability and Accountability Act (HIPAA). The law prohibits covered entities like hospitals from sharing personally identifiable health information with third parties like Facebook, except when an individual has expressly consented in advance or under certain contracts.

Neither the hospitals nor Meta said they had such contracts in place, and The Markup found no evidence that the hospitals or Meta were otherwise obtaining patients' express consent.

"I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it," said David Holtzman, a health privacy consultant who previously served as a senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, which enforces HIPAA. "I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA violation."

University Hospitals Cleveland Medical Center spokesperson George Stamatis did not respond to The Markup's questions but said in a brief statement that the hospital "comport[s] with all applicable federal and state laws and regulatory requirements."

After reviewing The Markup's findings, Froedtert Hospital removed the Meta Pixel from its website "out of an abundance of caution," Steve Schooff, a spokesperson for the hospital, wrote in a statement.

As of June 15, six other hospitals had also removed pixels from their appointment booking pages and at least five of the seven health systems that had Meta Pixels installed in their patient portals had removed those pixels.

The 33 hospitals The Markup found sending patient appointment details to Facebook collectively reported more than 26 million patient admissions and outpatient visits in 2020, according to the most recent data availablefrom the American Hospital Association. Our investigation was limited to just over 100 hospitals; the data sharing likely affects many more patients and institutions than we identified.

Facebook itself is not subject to HIPAA, but the experts interviewed for this story expressed concerns about how the advertising giant might use the personal health data it's collecting for its own profit.

"This is an extreme example of exactly how far the tentacles of Big Tech reach into what we think of as a protected data space," said Nicholson Price, a University of Michigan law professor who studies big data and health care. "I think this is creepy, problematic, and potentially illegal" from the hospitals' point of view.

The Markup was unable to determine whether Facebook used the data to target advertisements, train its recommendation algorithms, or profit in other ways.

Facebook's parent company, Meta, did not respond to questions. Instead, spokesperson Dale Hogan sent a brief email paraphrasing the company's sensitive health data policy.

"If Meta's signals filtering systems detect that a business is sending potentially sensitive health data from their app or website through their use of Meta Business Tools, which in some cases can happen in error, that potentially sensitive data will be removed before it can be stored in our ads systems," Hogan wrote.

Meta did not respond to follow-up questions, but Hogan appears to be referencing a sensitive health information filtering system that the company launched in July 2020 in response to a Wall Street Journal article and New York Department of Financial Services investigation. Meta told the investigators that the filtering system was "not yet operating with complete accuracy," according to the department's February 2021 final report.

The Markup was unable to confirm whether any of the data referenced in this story was in fact removed before being stored by Meta. However, a recent joint investigation with Reveal found that Meta's sensitive health information filtering system didn't block information about appointments a reporter requested with crisis pregnancy centers.

Internally, Facebook employees have been blunt about how well—or not so well—the company generally protects sensitive data.

"We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' " Facebook engineers on the ad and business product team wrote in a 2021 privacy overview that was leaked to Vice.

The Meta 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. It's one of the most prolific tracking tools on the internet—present on more than 30 percent of the most popular sites on the web, according to The Markup's analysis.

In exchange for installing its pixel, Meta provides website owners analytics about the ads they've placed on Facebook and Instagram and tools to target people who've visited their website.

The Meta Pixel sends information to Facebook via scripts running in a person's internet browser, so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.

HIPAA lists IP addresses as one of the 18 identifiers that, when linked to information about a person's health conditions, care, or payment, can qualify the data as protected health information. Unlike anonymized or aggregate health data, hospitals can't share protected health information with third parties except under the strict terms of business associate agreements that restrict how the data can be used.

In addition, if a patient is logged in to 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.

And in 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.

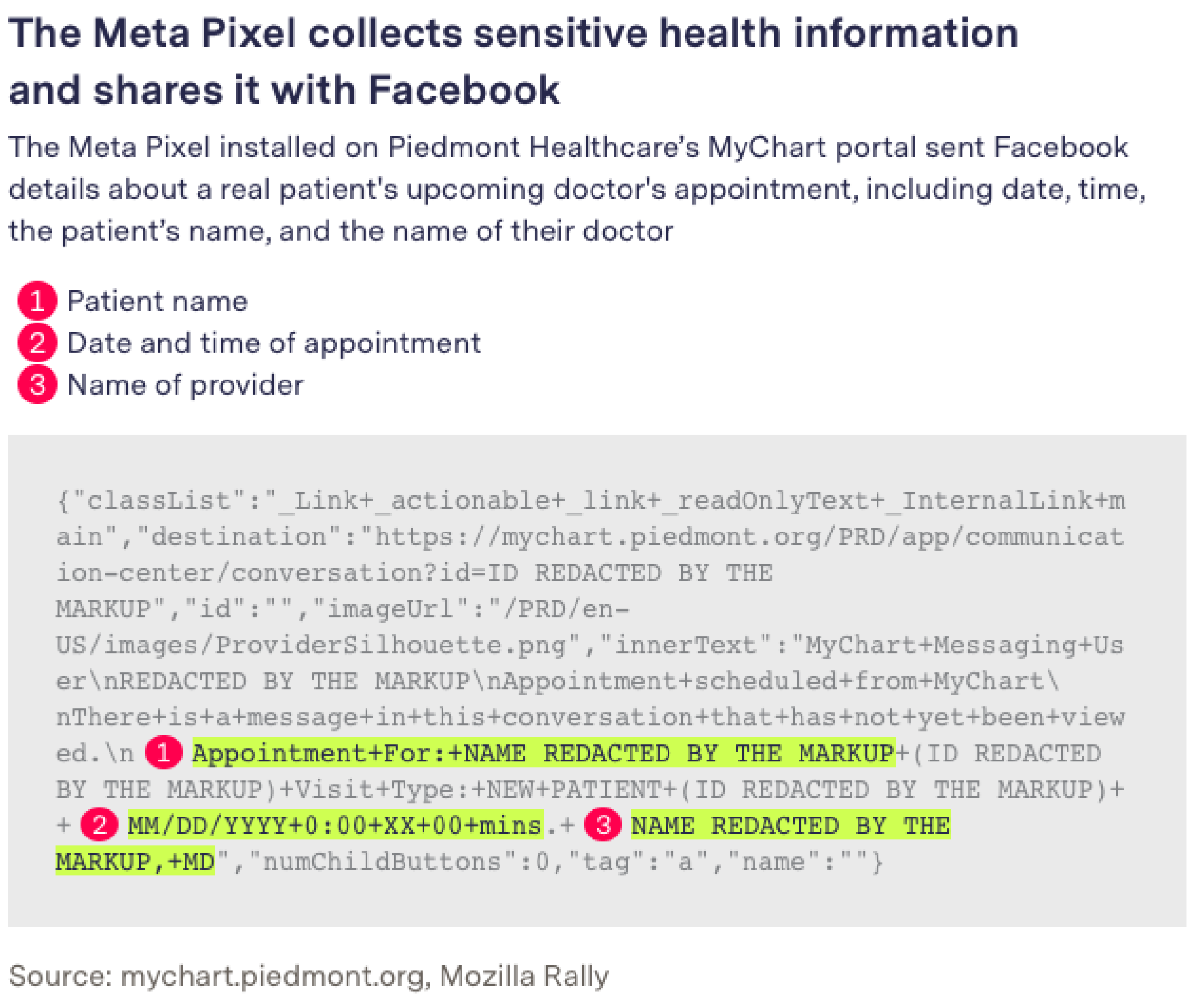
The Meta Pixel "hashed" those personal details—obscuring them through a form of cryptography—before sending them to Facebook. But that hashing doesn't prevent Facebook from using the data. In fact, Meta explicitly uses the hashed information to link pixel data to Facebook profiles.

Using a free online tool, The Markup was also able to reverse most of our hashed test information that the pixel on Scripps Memorial Hospital's website sent to Facebook.

Scripps Memorial didn't respond to The Markup's questions but it did remove the Meta Pixel from the final webpages in the appointment booking process after we shared our findings with the hospital.

On other hospitals' websites, we documented the Meta Pixel collecting similarly intimate information about real patients.

When one real patient who participated in the Pixel Hunt study logged in to the MyChart portal for Piedmont Healthcare, a Georgia health system, the Meta Pixel installed in the portal told Facebook the patient's name, the name of their doctor, and the time of their upcoming appointment, according to data collected by the participant's Mozilla Rally browser extension.



The Meta Pixel collects sensitive health information and shares it with Facebook

The Meta Pixel installed on Piedmont Healthcare's MyChart portal sent Facebook details about a real patient's upcoming doctor's appointment, including date, time, the patient's name, and the name of their doctor

① Patient name
② Date and time of appointment
③ Name of provider

```
{"classList":"_Link+_actionable+_link+_readOnlyText+_InternalLink+m
ain","destination":"https://mychart.piedmont.org/PRD/app/communicat
ion-center/conversation?id=ID REDACTED BY THE
MARKUP","id":"","imageUrl":"/PRD/en-
US/images/ProviderSilhouette.png","innerText":"MyChart+Messaging+Us
er\nREDACTED BY THE MARKUP\nAppointment+scheduled+from+MyChart\
nThere+is+a+message+in+this+conversation+that+has+not+yet+been+view
ed.\n ① Appointment+For:+NAME REDACTED BY THE MARKUP+(ID REDACTED
BY THE MARKUP)+Visit+Type:+NEW+PATIENT+(ID REDACTED BY THE MARKUP)+
+ ② MM/DD/YYYY+0:00+XX+00+mins.+ ③ NAME REDACTED BY THE
MARKUP,+MD","numChildButtons":0,"tag":"a","name":""}
```

Source: mychart.piedmont.org, Mozilla Rally

When another Pixel Hunt participant used the MyChart portal for Novant Health, a North Carolina-based health system, the pixel told Facebook the type of allergic reaction the patient had to a specific medication.

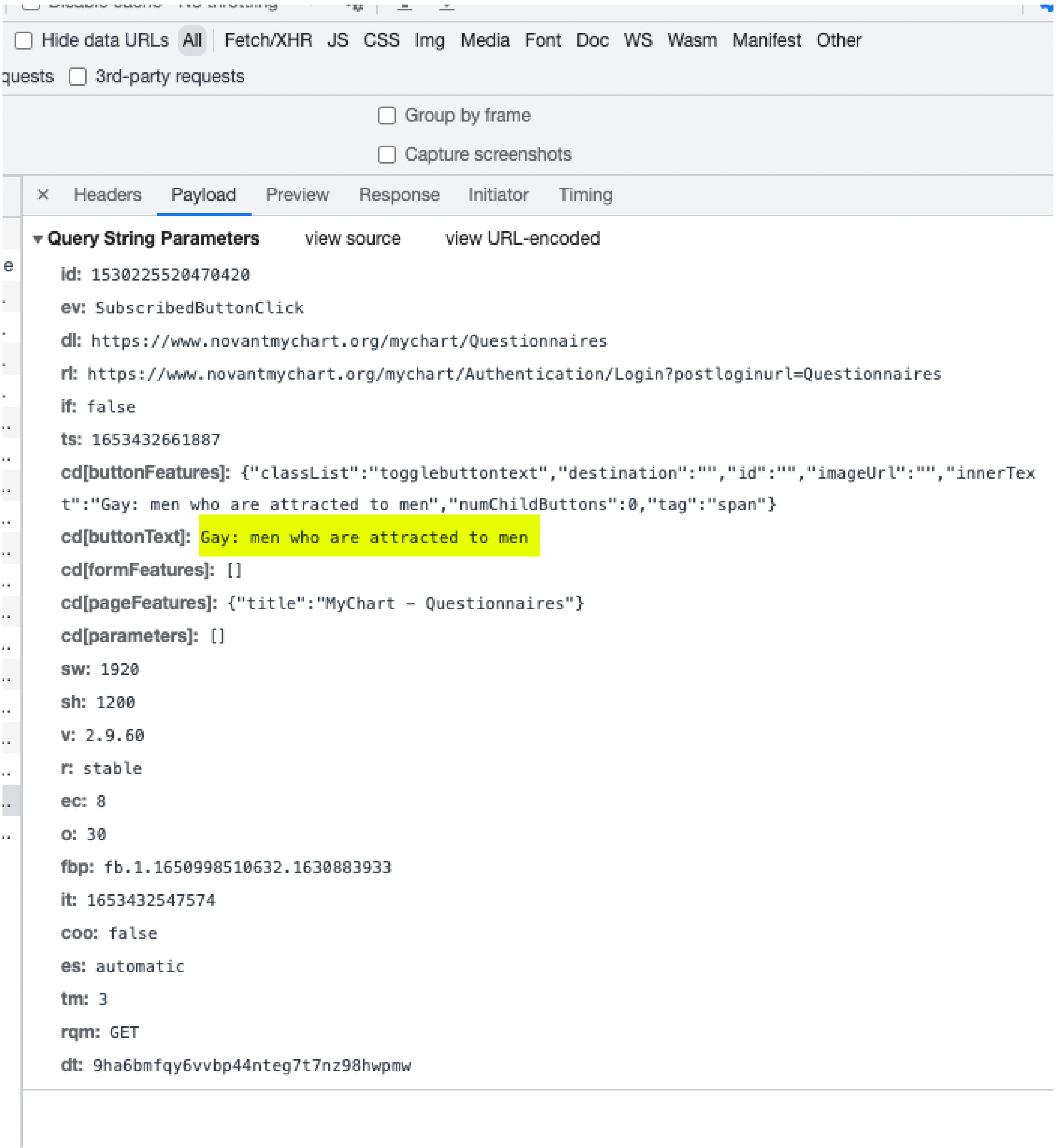
The Markup created our own MyChart account through Novant Health to further investigate and found the Meta Pixel collecting a variety of other sensitive information.

Clicking on one button prompted the pixel to tell Facebook the name and dosage of a medication in our health record, as well as any notes we had entered about the prescription. The pixel also told Facebook which button we clicked in response to a question about sexual orientation.

“Our Meta pixel placement is guided by a third party vendor and it has been removed while we continue to look into this matter,” Novant spokesperson Megan Rivers wrote in an email.

Epic Systems, the software company behind MyChart, has “specifically recommended heightened caution around the use of custom analytics scripts,” Stirling Martin, a senior vice president for the company, wrote in an email.

Facebook is able to infer intimate details about people’s health conditions using other means—for example, the fact that a person “liked” a Facebook group associated with a particular disease—but the data collected by pixels on hospitals’ websites is more direct. And in sharing it with Facebook, experts said, health care providers risk damaging patients’ trust in an increasingly digitized health system.



```
id: 1530225520470420
ev: SubscribedButtonClick
dl: https://www.novantmychart.org/mychart/Questionnaires
rl: https://www.novantmychart.org/mychart/Authentication/Login?postloginurl=Questionnaires
if: false
ts: 1653432661887
cd[buttonFeatures]: {"classList":"togglebuttontext","destination":"","id":"","imageUrl":"","innerTex
t":"Gay: men who are attracted to men","numChildButtons":0,"tag":"span"}
cd[buttonText]: Gay: men who are attracted to men
cd[formFeatures]: []
cd[pageFeatures]: {"title":"MyChart - Questionnaires"}
cd[parameters]: []
sw: 1920
sh: 1200
v: 2.9.60
r: stable
ec: 8
o: 30
fbp: fb.1.1650998510632.1630883933
it: 1653432547574
coo: false
es: automatic
tm: 3
rqm: GET
dt: 9ha6bmfqy6vvbp44nteg7t7nz98hwpmw
```

The Markup found that filling out a survey through Novant Health shared sensitive information like sexual orientation with Facebook via the Meta Pixel. Source: www.novantmychart.org

“Almost any patient would be shocked to find out that Facebook is being provided an easy way to associate their prescriptions with their name,” said Glenn Cohen, faculty director of Harvard Law School’s Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics. “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.”

Legal Implications

Facebook’s data collection on hospital websites has been the subject of class action lawsuits in several states, with mixed results.

Those cases involve types of data that health law experts said are sensitive but less regulated than the health information The Markup documented the Meta Pixel collecting.

In 2016, a group of plaintiffs sued Facebook and a handful of health systems and organizations, alleging that the organizations had breached their own privacy policies and several state and federal laws—including wiretapping and intrusion on seclusion statutes—by collecting data via tracking technology on the health care providers' websites.

The U.S. District Court for the Northern District of California dismissed that case in 2017 for a variety of reasons, including that the plaintiffs failed to prove that Facebook had collected "protected health information," as defined by HIPAA. Rather, the court found, Facebook had tracked plaintiffs on public-facing pages of the websites—such as the homepage or informational pages about diseases—where there was no evidence that the plaintiffs had established a patient relationship with the provider.

In 2019, plaintiffs brought a similar class action lawsuit in Suffolk County Superior Court against Massachusetts-based Partners Healthcare System, which has since changed its name to Mass General Brigham, alleging that the system had violated patients' privacy and its own policies by installing the Meta Pixel and other tracking tools on its websites.

The parties settled the case in January, with Mass General Brigham denying the allegations and admitting no wrongdoing or liability but paying $18.4 million to the plaintiffs and their attorneys. After the settlement, Mass General Brigham appears to have removed Meta Pixel and other tracking tools from many of its hospitals' websites—but not all of them.

When The Markup tested the website of Brigham and Women's Faulkner Hospital, clicking the "Request Appointment" button on a doctor's page caused the Meta Pixel to send Facebook the text of the button, the doctor's name, and the doctor's field of medicine. Mass General did not respond to The Markup's request for comment.

As with all such data we found the Meta Pixel collecting, it was sent to Facebook along with our computer's public IP address.

"When an individual has sought out a provider and indicated that they want to make an appointment, at that point, any individually identifiable health information that they've provided in this session, in the past, or certainly in the future, is protected under HIPAA and could not be shared with a third party like Facebook," Holtzman said.

The U.S. Department of Human Services' Office for Civil Rights "cannot comment on open or potential investigations," spokesperson Rachel Seeger wrote in an emailed statement.

"Generally, HIPAA covered entities and business associates should not be sharing identifiable information with social media companies unless they have HIPAA authorization [from the individual] and consent under state law," said Iliana Peters, a privacy lawyer with the firm Polsinelli who previously headed HIPAA enforcement for the Office for Civil Rights.

Patients have the right to file HIPAA complaints with their medical providers, who are required to investigate the complaints, Peters said, adding, "I would hope that institutions would respond quickly to those types of complaints so that they aren't escalated to a state or federal regulator."

“Plausible Deniability“

Most of the hospitals The Markup contacted for this story did not respond to our questions or explain why they chose to install Meta Pixel on their websites. But some did defend their use of the tracker.

“The use of this type of code was vetted,” wrote Chris King, a spokesperson for Northwestern Memorial Hospital, in Chicago. King did not respond to follow-up questions about the vetting process.

King said that no protected health information is hosted on or accessible through Northwestern Memorial’s website and that “Facebook automatically recognizes anything that might be close to personal information and does not store this data.”

In fact, Meta explicitly states in its business tools terms of service that the pixel and other trackers do collect personally identifiable information for a variety of purposes.

Houston Methodist Hospital, in Texas, was the only institution to provide detailed responses to The Markup’s questions. The hospital began using the pixel in 2017, spokesperson Stefanie Asin wrote, and is “confident” in Facebook’s safeguards and that the data being shared isn’t protected health information.

When The Markup tested Houston Methodist’s website, clicking the “Schedule Appointment” button on a doctor’s page prompted the Meta Pixel to send Facebook the text of the button, the name of the doctor, and the search term we used to find the doctor: “Home abortion.”

Houston Methodist doesn’t categorize that data as protected health information, Asin wrote, because a person who clicks the “Schedule Appointment” button may not follow through and confirm the appointment, or, they may be booking the appointment for a family member rather than for themself.

“The click doesn’t mean they scheduled,” she wrote. “It’s also worth noting that people often are exploring for a spouse, friend, elderly parent.”

Asin added that Houston Methodist believes Facebook “uses tools to detect and reject any health information, providing a barrier that prevents passage of [protected health information].”

Despite defending its use of the Meta Pixel, Houston Methodist Hospital removed the pixel from its website several days after responding to The Markup’s questions.

“Since our further examination of the topic is ongoing, we elected to remove the pixel for now to be sure we are doing everything we can to protect our patients’ privacy while we are evaluating,” Asin wrote in a follow-up email.

Facebook did not launch its sensitive health data filtering system until July 2020, three years after Houston Methodist began using the pixel, according to the New York Department of Financial Services’ investigation. And as recently as February of last year, the department reported that the system’s accuracy was poor.

That type of Band-Aid fix is a prime example, privacy advocates say, of the online advertising industry’s inability to police itself.

"The evil genius of Facebook's system is they create this little piece of code that does the snooping for them and then they just put it out into the universe and Facebook can try to claim plausible deniability," said Alan Butler, executive director of the Electronic Privacy Information Center.

> "The fact that this is out there in the wild on the websites of hospitals is evidence of how broken the rules are."

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

This article was copublished with STAT, a national publication that delivers trusted and authoritative journalism about health, medicine, and the life sciences. Sign up for their health tech newsletter, delivered Tuesday and Thursday mornings, here: https://www.statnews.com/signup/health-tech/

Featured image is from The Markup

The original source of this article is The Markup

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Todd Feathers**,
Simon Fondrie-Teitler,
and **et al.**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca