All Eyes On Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems

Mingjia Huo
University of Illinois Urbana-Champaign
Champaign, Illinois, USA
mhuo4@illinois.edu

Maxwell Bland
University of Illinois Urbana-Champaign
Champaign, Illinois, USA
mb28@illinois.edu

Kirill Levchenko
University of Illinois Urbana-Champaign
Champaign, Illinois, USA
klevchen@illinois.edu

Abstract

In the United States, sensitive health information is protected under the Health Insurance Portability and Accountability Act (HIPAA). This act limits the disclosure of Protected Health Information (PHI) without the patient's consent or knowledge. However, as medical care becomes web-integrated, many providers have chosen to use third-party web trackers for measurement and marketing purposes. This presents a security concern: third-party JavaScript requested by an online healthcare system can read the website's contents, and ensuring PHI is not unintentionally or maliciously leaked becomes difficult. In this paper, we investigate health information breaches in online medical records, focusing on 459 online patient portals and 4 telehealth websites.

We find 14% of patient portals include Google Analytics, which reveals (at a minimum) the fact that the user visited the health provider website, while 5 portals and 4 telehealth websites contained JavaScript-based services disclosing PHI, including medications and lab results, to third parties. The most significant PHI breaches were on behalf of Google and Facebook trackers. In the latter case, an estimated 4.5 million site visitors per month were potentially exposed to leaks of personal information (names, phone numbers) and medical information (test results, medications). We notified healthcare providers of the PHI breaches and found only 15.7% took action to correct leaks. Healthcare operators lacked the technical expertise to identify PHI breaches caused by third-party trackers. After notifying Epic, a healthcare portal vendor, of the PHI leaks, we received a prompt response and observed extensive mitigation across providers, suggesting vendor notification is an effective intervention against PHI disclosures.

CCS Concepts

• **Security and privacy → Web application security**; **Human and societal aspects of security and privacy**.

Keywords

web tracking, web privacy, HIPAA, protected health information

WPES '22, November 7, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9873-2/22/11…$15.00
https://doi.org/10.1145/3559613.3563190

ACM Reference Format:
Mingjia Huo, Maxwell Bland, and Kirill Levchenko. 2022. All Eyes On Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES '22), November 7, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3559613.3563190

1 Introduction

Health is moving online. In 2020, the Office of the National Coordinator for Health IT [43] reported that 6 in 10 individuals in the U.S. had access to their Electronic Health Record (EHR), and 4 in 10 accessed their health records at least once, an 11% increase from 2017. Moreover, 83% of these users access an EHR portal using a web browser. This is happening in the midst of a proliferation of *web trackers*—services that track user behavior on the web for analytics and advertising [33]—putting health care providers' compliance with privacy regulations on a collision course with modern web practices.

As we show in this work, many online health care providers use third-party trackers on their web sites, including parts of their sites that display and manipulate patients' health information. We found that common trackers such as Facebook Pixel and Google Analytics disclose protected health information (PHI) to Facebook and Google, respectively. In the United States, such information is protected by the Health Insurance Portability and Accountability Act (HIPAA) [20] and associated regulations.

Specifically, we investigated PHI breaches in two types of online patient care systems: *Electronic Health Record (EHR) patient portals* (or *patient portals* for short), used by hospitals and clinics to allow patients to view their medical information, schedule care, and communicate with their providers; and *telehealth websites*, used to provide long-distance contact with clinicians. We discovered that 14% of 465 systems we studied leak some form of PHI to third-party services. We found disclosure of PHI, including laboratory test results, phone numbers, patient names, emails, medications, and plans of care to Facebook. We also found less severe, but still very troubling, disclosure of PHI of patients' browsing behavior (page titles and URLs) while interacting with providers' sites to Google.

To remedy this, we contacted the affected hospitals and telehealth services. Less than a quarter of hospitals and clinics notified responded to our notification, and only about a sixth removed trackers from their EHR sites. None of the telehealth providers responded or made changes to their sites. We later notified Epic, the most popular EHR vendor, of the problem. While Epic does not control providers' sites directly, they raised the issue with their users.

Their intervention was dramatically more effective than our notification: all Epic EHR portals we studied removed Facebook Pixel and 21% removed Google Analytics. We also reported this issue to the U.S. Department of Health and Human Services, the agency responsible for enforcing HIPAA regulations, and they informed us they are now actively looking into the issue.

In summary, we make the following contributions:

(1) A survey of Protected Health Information leaks to web trackers on patient health portals and telehealth websites. We found 5 patient portals and 3 telehealth providers leaked extensive medical information to Facebook. 67 EHR portals leaked at least the *fact* of visiting the portals, which indicates the *fact* of treatment, and in some cases additional information, to Google.
(2) A study on the impact of two interventions: direct notification by us and guidance from the EHR vendor. We found the latter to be more effective than the former, eliminating all use of Facebook Pixel among hospitals using the vendor's EHR, and reducing the use of Google Analytics by 21%.

The rest of the paper is organized as follows. Section 2 provides background on HIPAA, web tracking, and online health information. Sections 3 and 4 describe surveys of PHI disclosures in patient portals and telehealth websites, respectively. In Section 5, we discuss whether notification mitigates PHI disclosure by online health care systems. Section 6 discusses mitigation against PHI disclosure. We discuss related work in Section 7 and conclude in Section 8.

2 Background

2.1 Web Trackers

Today's websites commonly use web trackers to collect user browsing information [46]. Commonly-used trackers can be classified as being one of two types:

Tracking pixels. The simplest form of tracking is to embed an invisible one-pixel image in a Web page. In the past, such a request included the URL of the embedding page in the Referrer header, along with any cookies for the image's Web origin. (Today, browsers default to sending the requesting page's domain only.) By setting a persistent, uniquely identifying cookie, a tracker can observe all tracked pages visited by a particular user.

JavaScript. Most modern web browsers support JavaScript, which is loaded using a `<script>` HTML tag. Once loaded this way, the script is treated as belonging to the same origin as the containing page. As such, the third party script has access to all page contents via the Document Object Model (DOM). JavaScript may also make network requests to websites other than the one the user is currently browsing. If a JavaScript tracker is loaded onto a web page containing PHI, it has the ability to leak sensitive information by reading the DOM and sending this information to third parties.

The two most popular trackers we found on EHR portals and telehealth Web sites are Google Analytics and Facebook Pixel. Both of these load JavaScript on the visited page that sends telemetry to Google and Facebook, respectively.

2.2 Cookie Policies

Trackers use cookies to track users across page loads and this practice can be regulated by web browsers. Cookies sent to a different domain than that of the page loaded are termed *third-party cookies* (also called *cross-site cookies*). In September 2019, Firefox moved to block third-party cookies by default [2], followed by Safari in March 2020 [3]. Chrome has been slow to follow: in January 2020, Google announced that their "intention is to do this within two years." As of this writing, third-party cookies are still enabled by default. Instead, Chrome allows individual cookies to specify whether they should be sent in a third-party request via the SameSite cookie attribute [5].

2.3 Referrer Policies

Third party services loaded via HTTP could also leak PHI via the *Referer*[1] HTTP header. The Referer header can include the full path of the URL visited, e.g. "a.com/b/c.html" or just the origin, "a.com", depending on the web-page and browser *referrer policy*. Since healthcare portals sometimes store sensitive information in the URL path, the referrer policy adopted when browsing a healthcare portal determines whether this header can leak PHI.

Since July 23, 2020, Chrome's default referrer policy has been *strict-origin-when-cross-origin*, which does not send path information when making cross-origin (third party) requests [40]. As of 2021, Firefox has trimmed all Referer paths to protect user privacy [35]. We checked Safari version 15.5 manually and found that it also trims Referer header paths. In Section 3, we were careful to only consider PHI leaks that occurred due to services sending out URL path information via alternative channels not blocked by modern browser privacy features. All of our PHI leak measurements were performed with a strict-origin referrer policy, which always removes the path from the Referer URL.

2.4 HIPAA

In the United States, medical information is protected by federal regulations that stem from the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA regulations require a health provider (e.g. a hospital) to obtain explicit patient consent to share a patient's health information that is personally identifiable, that is, that can be linked back to the patient. HIPAA patient consent regulations are built around three concepts: *health information*, *protected health information*, and *individually identifiable health information* (45 CFR §160.103). To start,

> *Health information* means any information, including genetic information, whether oral or recorded in any form or medium, that:
> (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

[1]This misspelling of "referrer" may be a classic example of technical debt. By the time the error was noticed, HTTP was already standardized by RFC 1945.

Thus, health information includes information created or received by a health provider related to the provision of health care to an individual, which in principle includes even the *fact* of providing health care.

Protected health information (PHI) is "individually identifiable health information" that is "transmitted by electronic media" or "maintained in electronic media," with certain exceptions that do not apply here. Finally,

> *Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and:
> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
> (i) That identifies the individual; or
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

HIPAA regulations prohibit the disclosure of PHI to third parties without explicit patient consent. However, HIPAA makes an exception for *de-identified* health information. HIPAA spells out one way to de-identify health information, and that is to remove individual identifiers, including *name, phone number, email address, medical record numbers, account numbers, device identifiers, and serial numbers, Web URLs, IP addresses, any other unique identifying number, characteristic, or code* (45 CFR §164.514). In practice, this is interpreted to mean that any one of these identifiers makes protected health information identifiable [17]. By this definition, any electronically-transmitted health information that includes the patient's IP address is PHI.

Third-party trackers on health care websites run afoul of HIPAA because HTTP requests by trackers are made by the patient's browser, thus associating the patient's IP address with the information sent to the tracker. Cookie information sent by these services can also make browsing information personally identifiable. Chrome, which has 2/3 of the browser market share at the time of writing, allows third party trackers to send their host domain third party cookies. Google Analytics, for example, will include a user login *session cookie* in the tracker's requests to google.com if the user is logged into Google services. This makes any information sent to google.com by Google Analytics potentially personally identifiable, independent of whether the IP address is personally identifying. Even if the session cookie value does not contain PHI, the value is associated to the user's account identity in order to ensure the user can stay logged in to their Google account during a browsing session.

From our correspondence with healthcare providers that included trackers on their portals, it appears that many do not realize that the telemetry data sent to trackers is personally identifiable by virtue of the IP address and session cookies (Sec. 5.1.3).

2.5 Online Health Information

This paper studies PHI leaks in Electronic Health Record (EHR) portals and telehealth websites. In both cases, health information is hosted on an app or website. The form and type of information leaked depends on the website's functionality.

EHR portals are used by patients and health care providers for remote health information exchange and access. In the common case, portals are designed by an EHR brand, such as Epic MyChart, and included as part of a larger Electronic Medical Record solution. The portal website is usually customized for the provider from a template by adding provider-specific graphics and adding/removing features. These features can include systems for communicating with physicians, accessing medical results, transferring information between health care providers, and paying hospital bills. Section 3 finds several features which can leak both non-medical and medical PHI in MyChart and other portals.

Telehealth websites provide methods for scheduling medical appointments and may also include systems for accessing information about potential treatment locations. In order to provide remote treatment, these sites often include web forms for supplying PHI, e.g. reporting symptoms. In Section 4, we find PHI leaks through web trackers embedded in these remote care mechanisms. These services have also seen recent growth: during the COVID-19 pandemic, 64 percent of U.S. households reported receiving telehealth care [18].

3 PHI Leaks on Patient Portals

3.1 Methodology

Our study aims to determine what health information is sent to third-party services when interacting with health care providers' web sites. In this section, we examine one particular patient portal, Epic's MyChart [14], which has the largest market share (31%) [24, 42]. Epic lists the URLs of MyChart patient portals on its web site, making it easy to identify hospitals using MyChart.[2] We collected this MyChart list in September 2021.

Section 3.8 discusses and measures the prevalence of tracking in other EHR portals.

Registration. The Epic website includes a portal URL for every hospital using MyChart [14]. To evaluate whether these portals leak PHI through third-party services, we recorded web requests made by our browser when visiting pages of the site that displayed health information. This required logging into the EHR portal.

For 12 of the 459 MyChart patient portals, it was possible to register a user without any identity verification step, meaning that any internet user could create an anonymous account on the site. For the remaining 447 patient portals, some form of identity verification was required, either using a verification service provided by Equifax (a credit reporting agency) or through the use of a patient ID.

Because the identity verification step was time consuming, we measured the differences in third party requests between the *front pages* of each portal, the pages before login, and the *back pages* of each portal. We sampled 15 portals uniformly at random from the 447 portals that required identity verification and combined these with the 12 portals that required no identity verification to sign up

[2]We do not know if these 459 URLs represent all hospitals with public MyChart sites or a curated subset.

for, making a sample of 27 portals total. Excluding reCAPTCHA[3], only two portals had fewer third party services on their back pages.

The other 25 of the 27 MyChart patient portals had the same set of third party requests on the back pages of the website as on the front pages. In the remainder of this study, we report MyChart results based on front pages alone, unless noted otherwise. We expect 76.6%–97.9% (95% confidence interval, assuming 27 are independent) of all portals to have the same set of third-party services on the front and back pages.

Data Collection. We use OpenWPM[26] (v0.17.0) to automatically collect the HTTP traffic generated by a browser visiting health care websites with headless Firefox (Version 90). When performing collection, we set the browser to allow all cookies, and we disabled Firefox's Enhanced Tracking Protection and Do-Not-Track signal. We kept a consistent (stateful) browser profile between page visits during same-day experiments, but we used a fresh profile without any cookies or browsing histories for the next data-collection date. Despite all being made by Epic Systems, each MyChart portal is configured by the customer (health care provider). Thus, each must be monitored independently for third-party scripts.

The primary concern of this study is health information leaks via third party services. We therefore identified all third party services occurring on two or more of the 459 MyChart portals identified above. For each third party service identified, we determined whether any health information would leak to the third party when performing common operations on a MyChart patient portal using the 27 sites for which we registered above. These operations included checking lab results and changing personal information. For any third party leaks of PHI, we validated that the third party service behaved identically across all portals for which we could register.

3.2 Limitations

This part of our study examines only the 459 MyChart patient portals listed on the Epic Systems web site. There may be providers who use MyChart patient portals but are not listed on Epic's web site, and there may be providers who do not use MyChart and instead opt to use an alternative portal (Section 3.8). We do not claim, therefore, that the set of patient portals we examine are representative of any particular population. They do, however, represent a *large* sample, as the patient portals we examined cover several large providers with millions of patients, and the PHI leaks we observe affect tens of millions of patients (Table 3 alone covers over 30 million patients). In fact, three of the 67 providers using Google Analytics were in the 20 best hospitals ranked by U.S. News: Rush University Medical Center, Houston Methodist Hospital, and Penn Presbyterian Medical Center [41].

Second, from the 511 URL portals listed by Epic, we exclude 52 for which it was not possible to accurately measure the included third party services. Despite being listed on the Epic website, these 52 healthcare provider sites did not appear to provide access to a MyChart patient portal publicly.

Third, our study identifies many, but likely not all, the pieces of information that each third party script collects from a patient portal. We did not consider side channels, steganography techniques, or other covert information leaks; our results should be understood as a lower bound on the information leaked to third parties.

3.3 Ethics

Our IRB determined that our study did not involve human subjects, as no human subject's data was collected for the study. On portals that required identity verification, the senior author of this paper entered their own true information for identity verification. However, we did not introduce any medical information to the system: we removed all information from the account after confirming the existence of third party services on back pages and verified that the original information did not persist. Anyone with internet access could create an account on these sites and we did not exploit any special access or vulnerabilities to register.

3.4 Results

Table 1 shows the set of third-party services that made web requests from two or more providers' MyChart portals. The first column lists the service. The *Domain* column shows the domain to which the most sensitive information was sent. The *Front* column shows the number of portals on which the service was used on the front (login) page only, while *Back* column shows two numbers: the first, before the /, is the number of portals on which the service was also used on back pages. As noted in Section 3.1, we checked the back pages of 27 portals; the back page counts are a subset of these. The second number, after the /, is the number of those 27 sites that had loaded the service on the front page.

Based on our sample of the 27 portals, we estimate that 3/4 (95% CI) of the portals that make third-party requests from the front page also contact those same services on their back pages, excluding Google reCAPTCHA. For Facebook Pixel, because the amount of information leaked was so egregious, we confirmed that 5 portals that included this tracker on their front page also included it on their back pages. Google Analytics was by far the most popular third-party request and was often the only third-party request made by the portal. However, we found 13% of portals contacted five or more third-party services, and 2% of portals contacted more than 10 services.

A check mark or star in the *Cookie* column of Table 1 indicates that the domain listed in the *Domain* column set a unique identifier cookie.[4] Unique identifier cookies can include but are not only *session cookies*. Session cookies are deleted once the web browser is closed and are less likely to be used as a tracking mechanism [36].

A star in the *Cookie* column indicates that the cookie could be linked to a person via a session cookie. This can happen because the three companies listed with a star—Google, LinkedIn, and Facebook—also provide other services where the user is personally identifiable. Taking Google as an example, when the same session cookie that is sent from a MyChart portal is also sent from a Google page when the user is logged in to Google, the session identifier

[3]Google reCAPTCHA occurs on the front pages of 19 of these portals and on none of the back pages as it is designed to ensure login operations are performed by human beings rather than function as a tracker.

[4]We consider a cookie to be a *unique identifier cookie* if it appeared to have high entropy, was user-specific (the value was unique across different browser instances on different machines), and did not change once set—the same criteria used to determine unique identifier cookies in prior work [27].

Table 1: Third party services appearing on at least 2 MyChart portals. Many EHR portals leak URLs and title metadata and a few leak PHI. Services with a star next to them are connected to session IDs for logged-in accounts (are directly personally identifiable). The "front " and "back" columns denote services measured on the front page and services *explicitly confirmed* to exist on back pages, respectively.

Third-Party Services	Domain	Cookies	AJAX	# Portals		Leaks	
				Front	Back	URL	DOM
Facebook Pixel	facebook.com	★	✓	7	5 / 6	✓	✓
Google Analytics	analytics.google.com	★	✓	67	13 / 14	✓	·
LinkedIn Insight Tag	px.ads.linkedin.com	★	✓	2	1 / 2	✓	·
Google reCAPTCHA	google.com	★	✓	396	0 / 15	✓	·
Adobe DTM	adobedtm.com	·	·	3	0 / 0	✓	·
Qualtrics Site Intercept	qualtrics.com	·	·	2	1 / 1	✓	·
Crazy Egg	crazyegg.com	·	·	2	2 / 2	✓	·
Tealium	tealiumiq.com	✓	·	2	0 / 0	✓	·
Google Tag Manager	googletagmanager.com	·	✓	57	8 / 9	✓	·
DoubleClick (Google)	doubleclick.net	✓	✓	4	2 / 2	✓	·
Usabilla	usabilla.com	·	✓	4	0 / 0	✓	·
Tealium	tiqcdn.com	·	✓	4	0 / 0	✓	·
PIWIK	piwik.pro	·	✓	4	0 / 0	✓	·
DataDog	datadoghq.com	·	✓	3	0 / 0	✓	·
Krux	krxd.net	✓	✓	2	1 / 1	✓	·
CallRail	callrail.com	·	✓	2	0 / 0	✓	·
CallTrk	calltrk.com	·	✓	2	1 / 1	✓	·

can be associated to the Google user account identity, making any information sent from the MyChart portal to Google personally identifiable.

The *AJAX* column in Table 1 indicates whether at least one of the requests to the third party service was an AJAX request. Third party services which make AJAX requests have the ability to monitor page interactions and send this information to outside domains. Services without checkmarks in this column make only one request to a third party (at page load), and none thereafter.

For each third-party service, we also indicate what information it sent to the domain listed in the *Domain* column. Every request included, at a minimum, a Referer header, which gave the domain name of the patient portal. A check mark in the *URL* column indicates that the embedding page's URL was also sent to the listed third party service. For MyChart, the page URL determines the title, which only describes the section of the site being viewed; it does not contain medical information (cf. Sec. 4.2). A third-party request that only includes the origin tells the third party that a visitor was on the site, while a request that includes the full URL tells the third party which parts of the site a site visitor loaded. See Section 3.6 for further discussion.

A check mark in the *DOM* column indicates that some of the embedding page's content was sent. Only one service—Facebook Pixel—does this; we discuss it separately in Section 3.6.

3.5 PHI Leak Severity

Recall from the discussion in Section 2.4 that Protected Health Information (PHI) is health information that is personally identifiable. *Health information* is information created or received by a health care provider that relates to the health of the individual or the provision of health care to an individual. In principle, this includes the *fact* of receiving care. Health information is protected by HIPAA if it is personally identifiable, that is, if it can be linked to an individual.

As noted earlier, IP addresses are commonly considered personally identifying, and under this definition, any health information that also has the patient's IP address is PHI. The health information sent to third-party services, notably to web trackers, is also identifiable by virtue of the unique identifier cookies that web trackers use to track a user across web sites. To the extent that we want to consider degrees of personal identifiability, web tracker session cookies sent to services where a user may be logged in (e.g. Google, Facebook, and LinkedIn) are *more* personally identifying than IP addresses, because the company operating the tracker can identify the user without any additional information.

The health information sent to third parties when visiting a patient portal can also be ranked by severity of disclosure. The least severe is the hospital domain name, which is sent in the HTTP Referer field of every request. In principle, this still discloses a relationship between a patient and provider, and thus implies that the patient is likely receiving treatment from the provider. It is, perhaps, no different than seeing a patient walk into a clinic, however, the fact that such information can be collected at scale—along with how often a patient interacts with their health care provider—should be protected from disclosure to third parties. Loading *any* resource from a third party service on a patient portal is a form of PHI leak, albeit the least severe of the PHI leaks we observed.

Next, in increasing order of severity, is the disclosure of the URLs visited by a patient while navigating on the provider's MyChart

Table 2: Sizes of EHR portals with Facebook Pixel PHI leaks.

Hospitals	Physicians	Visitors/Mo.
Advocate Aurora Health	8100	2M
Community Health Network	2500	506K
Edward-Elmhurst Health	1900	613K
OhioHealth	800	797K
Premier Health	700	373K
Beaver Medical Group	200	116K
FastMed	200 clinics	72K

Table 3: EHR portals with Google Analytics PHI leaks.

Health Systems	Rank [6]	Hospitals	Patients
Bon Secours Mercy Health	14	50	10.3M
Texas Health	29	27	7M
Advocate Aurora Health	30	26	3M
SSM Health	36	23	2.2M
Hospitals	-	Beds	-
Beaumont Hospital-Royal Oak	12	1131	661K
OhioHealth Riverside	15	1059	130K
Duke University Hospital	24	957	41K
Houston Methodist Hospital	37	907	1.6M
Sarasota Memorial Hospital	53	839	1.3M
Ochsner Medical Center	64	767	876K
Univ. of Kansas Hospital	66	900	1.6M
Lehigh Valley Hospital	69	729	1.5M

site. While MyChart URLs do not reveal any specific medical information, they still reveal what a patient is doing, e.g. making an appointment or viewing test results. Google Analytics leaks the full URL of each page a user visits on a site, and thus falls into this disclosure category.

Therefore, we must make an additional distinction between third party services loaded on the front and back pages of a MyChart site. If a service is only loaded on the front page, then it will not disclose medical information that is stored in the URL during patient portal navigation. It will only disclose the fact the patient visited the MyChart site. If a service is loaded on the back pages of a site, then it can see a user's navigation activity, potentially leading to a more severe PHI disclosure.

One tracker, Facebook Pixel, sends extensive PHI to Facebook, as discussed below, and is in a leak severity category of its own.

3.6 Social Connections

In this section, we examine in more depth three web trackers listed in Table 1 with a ★ in the *Cookie* column, namely Google Analytics, Facebook Pixel, and LinkedIn Insight Tag. These are of special interest because the companies that provide these services also offer web services that know a user's identity. When a user is logged in to those companies' services, the session identifiers used by their trackers on the patient portal site can be linked to a user's real identity. The session identifiers are also sent with the telemetry sent to the trackers, adding another means (in addition to IP address) by which health information sent to trackers is personally identifiable. To confirm this fact, and to understand what information is sent, we examined these three trackers in greater detail. Finally, we also examine reCAPTCHA, which is present on the front page of many portals, to understand exactly how much PHI is leaked through this channel.

3.6.1 Google Analytics

The most popular third-party tracker is Google Analytics. To use Google Analytics, a web site operator adds a fragment of JavaScript provided by Google to their page. This script then sends telemetry to Google.

Telemetry. Among other pieces of information, Google Analytics sends the page URL and page title to Google in an AJAX request. Note that modern browsers only send the portal domain name in the *Referer* header when loading a third-party resource (Sec. 2.3), so Google Analytics' AJAX request provides more information than would be sent by loading a third-party resource only. MyChart does not pass sensitive information in URL parameters. The URL determines only what page the user is viewing, with titles such as "Test Results" and "Medications." Thus, Google will know what pages a patient is viewing on the MyChart site, but nothing of the page's content. Nevertheless, the set of pages viewed by a patient on their patient portal, along with how often they view them and how long they remain on the site, is indicative of how often a patient interacts with their provider, gets lab tests, makes appointments, and so on, which likely correlates with their health.

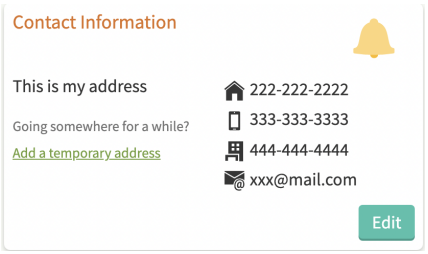
Identification. As noted in Section 2.4, IP addresses may be considered personally identifying, so any health information sent to Google is PHI. However, cookies used by web trackers provide another, easier way to link such information to a person. In the case of Google Analytics, the tracker script makes requests to the `google.com` domain and the `google-analytics.com` domain. Requests to `google.com` include Google's unique identifier cookies (`3PSID`, `3PAPISID`, `3PSIDCC`, and `NID`). These cookies have the *SameSite* attribute *None*, so they are sent by Chrome under its default cookie policy. (As discussed in Section 2.2, Firefox and Safari stopped sending third-party cookies in 2020.) We also confirmed that Google is indeed linking visits to the MyChart portals to a user identity by examining the account's activity history at `myactivity.google.com`, confirming that the telemetry sent to Google (described above) is indeed personally identifying.

3.6.2 Facebook Pixel

While Facebook's Pixel tracker was not the most common, it poses the most serious privacy concerns.

Telemetry. By default, Facebook Pixel sends fine-grained user interaction telemetry to Facebook. Specifically, when a user clicks on a page element, Pixel sends the contents of the page element to Facebook. Figure 1 shows an example of the data sent to Facebook when a user clicks on an element containing their address information. The request contains the complete contents of the element, notably the patient's phone number and email address.

Any information displayed to the patient is sent to Facebook if the user interacts with it. This is consistent with Facebook's own documentation [10]: "The Meta Pixel will send button click and



cd[buttonFeatures]: {"classList":"jqHidden differentHeights contact-information-content card withButton col-6 hover","destination":"","id":"contact-information-container","imageUrl":"/MyChart/en-US/images/PersonalInformation/phone_home.png","innerText":"Contact Information\nThis is my address\n\nGoing somewhere for a while?Add a temporary address\n222-222-2222\n333-333-3333\n444-444-4444\nxxx@mail.com","numChildButtons":3,"tag":"div"}
cd[buttonText]: Contact Information
This is my address

Figure 1: One web form which, when clicked, leaks PHI through Facebook Pixel. Pixel leaks PHI throughout EHR websites.

page metadata (such as data structured according to Opengraph or Schema.org formats) from your website to improve your ads delivery and measurement and automate your Pixel setup."

We found the following information can be leaked to Facebook servers from patient portals: personal information (name, address, phone number, email, gender, and birthday), medications (drug name and dosage), plans of Care (upcoming lab tests and prior results), appointments, (dates, hospitals, and topics).

We were able to register for an account on six of the seven patient portals listed in Table 1. Five of these six portals loaded Facebook Pixel on the back pages, meaning that their patients' detailed health information was being sent to Facebook.

Identification. Like Google Analytics, Facebook Pixel makes requests to the primary domain (`facebook.com`) and sends several unique identifier cookies with the *SameSite* attribute *None*. Moreover, if a Facebook user is logged in, Pixel also sends the Facebook user identifier in `c_user` parameter of the GET request made by Pixel to collect telemetry. We also confirmed that our visits to patient portals were listed in the activity section of the Facebook web site at `https://www.facebook.com/off_facebook_activity`.

3.6.3 LinkedIn Insight Tag

LinkedIn Insight Tag is a tracker similar to Google Analytics. We found only two hospitals loaded Insight Tag on their front page. Of these two, one also loaded it on back pages. Like Google Analytics, LinkedIn Insight Tag sends the page URL to LinkedIn. The telemetry is sent to `linkedin.com` along several unique identifier cookies (`_guid`, `li_sugr`, `lms_analytics`) [12] with the *SameSite* attribute *None*. Because LinkedIn does not provide a way for users to see their off-LinkedIn activity, we were not able to confirm that the telemetry sent by Insight Tag was internally associated with the user's account. However, because the unique identifier cookies are sent to LinkedIn when a user interacts with the main LinkedIn site, they can be associated with the user account.

3.6.4 Google reCAPTCHA

Google reCAPTCHA is a CAPTCHA service operated by Google. It appeared on the front pages (and only on the front pages) of 396 (86%) out of the 459 MyChart portals we examined. While reCAPTCHA is not ordinarily considered a web tracker, it makes a GET request to `google.com`. While the request URL does not contain any sensitive parameters, it does send the site domain name in the referrer. The request sends the same cookies to `google.com` as Google Analytics. These are the same cookies sent to `google.com` when the user interacts with Google directly, allowing Google to associate the cookies with the user's identity.

There is a belief that Google states that it does not use reCAPTCHA data for advertising. However, we were only able to find this statement for Google's reCAPTCHA *Enterprise* product [11]. In Section 6.2 we perform an experiment to determine whether Google associates reCAPTCHA data with user identities.

3.7 Estimating Affected Population

We sourced statistics from affected healthcare provider websites in order to estimate the patient population affected by the discovered PHI leaks. Table 2 lists the number of physicians for the seven hospitals using the Facebook Pixel tracker on the front page. We were also able to determine approximately 4.5 million site visitors per month were exposed to Facebook Pixel leaks. Based on a 2021 survey of the largest 100 hospitals in the U.S. [41], we were able to find exact patient population information for providers with portals containing Google Analytics. We give population measures for 12 major providers in Table 3, consisting of 4 health systems and 8 hospitals. While Google's PHI breaches were less severe than those of Facebook Pixel, they affect a larger number of patients overall.

3.8 Other Patient Portals

In addition to Epic's MyChart, which has the largest market share (31%) of patient EHR portals, we also examined other vendor's portals, covering an additional 40 providers. We sourced a list of popular EHR vendors and their relative market shares from a 2020 survey [30]. Unlike Epic's MyChart, there is no official list of providers using these portal brands. To find these portal websites, we entered each vendor's name into Google and identified all EHR portals occurring on the first five pages of search results. Below, we report our findings for each vendor (their market share is shown in parentheses):

Cerner (25%)**.** We note the only difference between provider's portals is a number in the portal's URL (a hospital ID). All Cerner portals contained the same third-party services: CloudFront for image hosting, Google JavaScript libraries, and `newrelic.com`. The former two did not create any network traffic to third parties, but the last one sent page view information and user identification cookies. However, New Relic claims to be a HIPAA compliant third-party.

MediTech (16%)**.** Of the 20 MediTech's EHR portals, none included third-party services.

Table 4: PHI leak distribution for four major telehealth providers. Direct leaks of PHI through the HTML DOM were more severe for telehealth providers than patient portals.

Third Party Service	Cookies		AJAX	URL	DOM
Google Analytics	★	3	4	4	1
DoubleClick	✓	3	3	3	1
Facebook Pixel	★	3	3	3	3
Microsoft UET	★	3	3	3	1
Heap Analytics		0	1	1	1
LinkedIn Ads	★	1	1	1	0
Reddit Pixel	★	1	1	1	0
Twitter Analytics	★	1	1	1	0

CPSI (9%)**.** All CPSI hosts redirected to a single domain which included third-party JavaScript services, but none sent cookies to third parties.

Allscripts (5%)**.** Allscripts portals included Google Analytics. A single Google Analytics Tracking ID was used across Allscripts sites, indicating they were centrally monitored.

eClinicalWorks (less than 5%)**.** Similar to Cerner, eClinicalWorks URLs were based on a hospital ID. However, the portals were not identical: 47% had Google Analytics on the front pages, 26% included third party services for Healow, a different health care application. Pages including these services sent cookie information to third parties. In February 2022, we observed that third-party services were removed from all eClinicalWorks websites.

NextGen (less than 5%)**.** All NextGen hosts redirected to `nextmd.com`. This site downloaded Google Analytics and JQuery.

Athenahealth (less than 5%)**.** All Athenahealth websites loaded an analytics tool from Amplitude. This service sent page metadata and browser fingerprints to Amplitude servers, and stored cookies containing unique user IDs inside the client's browser.

4 PHI Leaks On Telehealth Sites

4.1 Methodology

We expanded the domain of our research to include four telemedicine websites. To select the telehealth services to study, we performed a Google search for "best telehealth provider". We then selected four providers appearing in the first two search result links: Sesame, Amwell, MDLive, and Plushcare, as recommended by [7, 8]. We found that these search-engine recommended telehealth providers' websites all have PHI leaks.

We use the same methodology as in our study of patient portals, with modifications to how we browsed the websites to identify PHI leaks. No telehealth site required identity verification during registration. For each telehealth site, we edited our personal information on the site, accessed medical and medication records, and attempted to book an appointment. When accessing appointment bookings or medical records, we did not submit any service requests that would provide medical information to these providers. Figure 2 depicts an example of telehealth provider third party leaks we discovered.

4.2 Results

Overview. All the telehealth websites studied leak PHI to third parties. The telehealth sites contained trackers from popular third parties, shown in Table 4. All of the trackers in Table 4 leak page URL and visit telemetry. Compared to MyChart portals, telehealth site URL paths include more severe PHI leaks, including health condition, location, and lab test information.

The columns in Table 4 have identical descriptions to those of Section 3.4. Table 4 gives the number of telehealth portals affected for each PHI leak type. Unlike MyChart portals, we were able to register for all four telehealth sites and measure the exact amount of PHI leaked by each tracker on each site.

With the exception of Heap Analytics, the trackers in the table all belong to social media companies. The social media company trackers all included unique identifier cookies in their HTTP requests. DoubleClick and Facebook Pixel even include patients' inferred longitude and latitude in their requests. As previously mentioned, these unique identifier cookies can be used to identify the user (Sec. 3.4).

We found one telehealth site leaked PHI directly to Google Analytics (see Figure 2 for the discovered leak). This is a feature of Google Analytics [4] and was configured by the telehealth provider. This makes Google Analytics PHI leaks more severe for telehealth providers than EHR portals in the degree of health information revealed. At the time of writing, no MyChart portals leak HTML DOM information to Google Analytics (Sec. 3.6.1).

PHI Leak Analysis. The information leaks for telehealth sites were more severe than for patient portals. Below we include details on the information leaks for the four telehealth providers studied.

Amwell. Amwell sends URLs and HTML page titles including health record information, e.g. "Health Record: Blood Pressure", and unique identifier cookies due to the Google Analytics service.

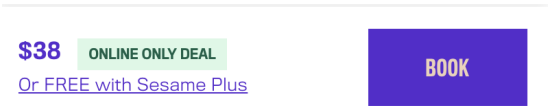
Sesame Care. Sesame Care leaks two forms of PHI when patients book a lab test or healthcare appointment (Figure 2). Google Analytics, DoubleClick, Facebook Pixel, and Microsoft's Universal Event Tracking leak lab test type and testing location information. Google Analytics, DoubleClick, and Facebook Pixel leak appointment dates, topics, and the health provider name.

MDLIVE. MDLIVE leaks both chronic and specific health condition information, such as allergies and symptoms, when patients check their "Health Profile" or schedule a physician appointment. This information is sent to facebook.com via the Facebook Pixel tracker.

PlushCare. PlushCare leaks several forms of information via the Heap Analytics service. This includes personal information: the patient's name, gender, insurance provider, and the last 4 digits of their credit card number. The Heap Analytics service also leaks patients' health provider histories, prescriptions, test results, and appointment topics, e.g. "Anxiety". These leaks occur when users interact with the "View History", "Prescriptions", "Tests & Results", "Your Health", and "Book an Appointment" site components.

5 Taking Action

HIPAA regulations impose strict requirements on PHI disclosure and many hospitals have dedicated staff to ensure compliance. We were surprised by both the number of sites leaking PHI and the



(a) Button to Book Lab Tests

```
ea: Book Appointment Clicked
el: HIV lab test | $38 | Quest Diagnostics , null
ev: 38
```

(b) Data sent by Google Analytics

```
cd[service_price]: 38
cd[service_date]: "2022-02-28T00:00:00.000Z"
cd[service_day_of_week]: Monday
cd[service_month]: February
cd[service_start_time]: 18:36:00
cd[content_ids]: 9c5fb6799b338c429e1cf3a7cbfe82e7
cd[content_type]: product
cd[product_type]: Call to schedule
cd[label]: HIV lab test | $38 | Quest Diagnostics , null
```

(c) Data sent by Facebook Pixel

Figure 2: Example of data sent by Google Analytics and Facebook Pixel by when booking a lab test with Sesame Care, the lab test name, inferred location (not shown in the figure), time, and price are sent to third parties.

severity of some leaks (Facebook Pixel). Nevertheless, we suspected that many providers did not realize that the information sent to third party services is personally identifiable via IP addresses and cookies. If ignorance is the cause, then informing health care website operators might be the cure. This section describes our efforts to get healthcare providers to remove third party trackers from their sites.

Our first line of attack was to notify providers directly. As discussed in Section 3.5, PHI leaks varied in severity. For our notification, we selected the two most troubling trackers, namely Facebook Pixel and Google Analytics. Unfortunately, our notification had negligible effect. For MyChart portals, we also notified Epic Systems, the developer of MyChart. While Epic itself is not responsible for individual providers' websites, they did issue guidance to their customers, which was more effective (Sec. 5.1.4). Finally, we also notified the US Federal Trade Commission and the US Department of Health and Human Services Office of Civil Rights; the latter is the regulatory agency in charge of HIPAA enforcement.

5.1 MyChart Portals

5.1.1 Methodology

Providers. As noted above, we chose to notify providers that had Facebook Pixel or Google Analytics on their site, as we judged these two trackers to be the most severe form of PHI leaks. However, as discussed in Section 3.1, we could not examine the back pages of all MyChart sites, and, therefore, could not determine whether Google Analytics code was present on back pages (pages after login). Having Google Analytics present on back pages leaks substantially more information than on the front page alone (Sec. 3.5). We elected to contact all providers with Google Analytics or Facebook Pixel on their *front pages*.

Contact address. Our next step was to determine whom we should contact at a given provider. Hospitals generally had up to three possibilities for electronic contact:

- *IT.* The IT department that is responsible for operating the MyChart portal is directly responsible for code appearing on the provider's MyChart site. Based on the handful of responses we received, it is likely that they added the tracker code to their site in order to get site analytics.
- *Privacy/compliance.* Many providers had a compliance or privacy office or officer whose contact information was listed on the provider's site. They are responsible for ensuring HIPAA compliance.
- *Generic contact form.* Many providers also had a generic *Contact Us* form on their site.

For each provider, we first attempted to determine all the available means of contact, and then classified each potential recipient into one of the three categories above. We decided that the first two, IT and privacy/compliance, would be more effective than the generic contact form,[5] and elected to initiate contact with one of the first two in preference over the third. If a provider had both an IT and a privacy/compliance contact, we *selected randomly between the two.* This would allow us to determine which of the two recipients is a more effective contact for such notifications—potentially a useful result for future actions of this kind.

We notified the privacy/compliance office of 26 providers, the IT contact of another 31, and the general contact form of another 13 (70 total).

Notification letter. On December 14, 2021, we sent the notification letter, shown in full in Appendix A, to providers with MyChart portals that had Facebook Pixel or Google Analytics.

Monitoring. We collected a snapshot of MyChart portals' front page third-party requests on September 29, 2021 and then again on December 14, 2021, immediately prior to sending our notification. After notifying the providers that use MyChart, as described above, we monitored providers' MyChart portals for changes in the set of trackers they loaded. In addition, we also monitored their privacy policies for changes after notification. We collected two snapshots, on February 25, 2022 and on July 5, 2022.

5.1.2 Results

Tracker Use. Table 5 shows the popularity of third party trackers on MyChart front-pages before and after notification. In parenthesis we include the relative change in service populations across time; these numbers indicate the number of unique portals that added or removed trackers. Before notification, the frequency of Google

[5] Our reasoning was that the generic contact form would receive a large volume of messages, including medical care and billing, so our notification would be more likely to get lost.

Table 5: Number of MyChart portals including four types of third-party code. Providers were notified directly immediate after the December 14, 2021 data was collected.

Third-Party Script	Sep. 29	Dec. 14	Feb. 25	Jul. 5
Google Analytics	67	68 (+2, −1)	63 (+3, −8)	45 (+3, −21)
Google Tag Manager	57	55 (+0, −2)	53 (+2, −4)	39 (+2, −16)
Facebook Pixel	7	6 (+0, −1)	5 (+2, −3)	0 (+0, −5)
DoubleClick	4	3 (+0, −1)	5 (+2, −0)	4 (+1, −2)

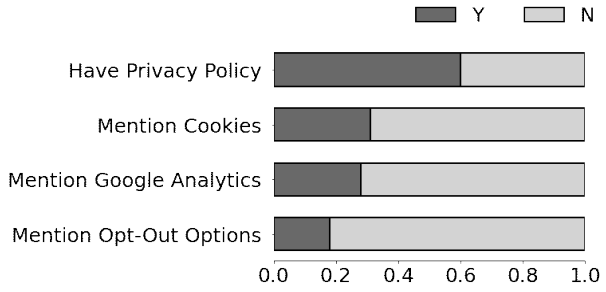


Figure 3: Relative frequency of privacy policy inclusions in the 70 notified healthcare providers with third party PHI leaks.

Analytics and Facebook trackers was approximately unchanged. After our notification, 8 hospitals removed Google Analytics and 3 hospitals removed Facebook Pixel.

We found any positive changes as a result of our notification were offset by the influx of added trackers. After notification, two providers added Facebook Pixel to their EHR portals: Houston Methodist and WakeMed. Surprisingly, Houston Methodist was one of the sites we notified, as on December 14th their EHR portal included Google Analytics. Our conclusion is that direct notification was ineffective at stopping PHI leaks.

Privacy Policies. Of the 70 health providers notified in the previous section, we recorded whether they provided a privacy policy. If the provider had a privacy policy, we measured whether the provider's privacy policy mentioned the existence of third party services and whether it provided a mechanism to opt out of third party data collection. Note that mentioning third-party trackers in a privacy policy does *not* satisfy HIPAA requirements for affirmative consent to share information. Nevertheless, disclosing third-party data sharing is better than not disclosing third-party data sharing.

In our notification email to providers without a privacy policy or without a policy mentioning third-party services, we included the following text: "When we accessed your website, we were not asked for consent to share health information with *(companies*), nor did your website provide any indication that the information above is being sent to *(companies*)." We might expect, therefore, that our notification would have the effect of at least moving providers to update their privacy policies.

Figure 3 gives proportional results for the privacy policies of 70 healthcare providers. 39 MyChart portals contained privacy policies, 29 of which redirected to the healthcare provider's primary website. 30.7% of privacy policies mentioned the existence of third-party cookies. Among the ones that mention third-party cookies, 28.2% mentioned Google Analytics, and 17.9% provided methods of opting out of cookies and tracking. Of the 5 privacy policies for portals including Facebook Pixel, none mentioned the tracker or transmission of PHI to third parties.

After our December 14, 2021 notification event, we monitored each provider for privacy policy changes. Over two months, we detected the addition of a single privacy policy: Children's Wisconsin added a privacy policy to their MyChart portal [16]. This policy discussed the data collected by their portal, including third-party cookies. Providers UC Health and Salem Heath added information to their existing policies. UC Health added a paragraph on information collected by their MyChart portal's mobile app.

Thus, we find mentioning a lack of user consent to share information with third parties when informing healthcare providers about health information leakages had neglilgible effect on those providers' privacy policies.

5.1.3 Individual Providers' Responses

Only 16 out of 70 providers we notified sent responses. The healthcare providers that responded showed differing attitudes and solutions to the privacy violations created by third-party service inclusion. Nine of these replies claimed they would or had mitigated any PHI information breaches. One provider claimed to not have third party trackers on the back pages of their EHR portal. In order to provide insight into providers' perspectives on this issue, we present three responses here. All three responses were cordial.

Response 1. One healthcare provider notified us they examined the information leaked by Google Analytics, *contacted Epic about the leak*, and discussed the matter internally. They communicated to us that only basic, de-identified information is sent to Google: session location, time, and frequency. They informed us that no patient information on their portal was shared with third parties. We found this provider removed Google Analytics within 2 days of sending a response.

Response 2. The security officers confirmed that although their EHR portal landing page has Google Analytics, there is no such code beyond the login page for the privacy reasons our notification letter mentioned. They indicated their marketing team uses the tracker to determine the effectiveness of out-reach initiatives.

Response 3. A third provider removed Google Tag Manager (GTM) after our notification. They also mentioned a plan to remove GTM from post-login pages only, in order to provide marketing analytics for an "open scheduling widget", and mentioned interest in a mechanism for determining if PHI breaches exist after performing website third party service inclusion updates.

These responses indicate that some healthcare providers are aware of the privacy risks involved with third-party trackers. The responses also suggest some providers utilize trackers for explicit marketing purposes. Under the HIPAA Breach Notification Rule, healthcare providers must inform patients of data breaches [1]. Facebook Pixel leaked PHI on both MyChart portals and telehealth websites. However, we did not observe any notification process on behalf of the affected healthcare providers by checking for emails received by the primary email inbox and spam inbox of the account used to register for portal websites.

5.1.4 Actions by Epic Systems

On June 16, 2022, we contacted MyChart developer Epic Systems to alert them to their customers' use of third party trackers. While Epic is not responsible for their customer's use of trackers, the limited effect of our own notification efforts led us to pursue this option as well. Epic responded that they had raised this concern with their customers on June 1, 2022, and have observed that "at least 60% of the sites where we'd observed Facebook Pixel potentially in use discontinued it, and at least 17% of the sites where we'd observed Google Analytics in use discontinued it." We note this response on the behalf of providers and Epic may have been spurred by a contemporaneous media article regarding Facebook Pixel trackers on hospital websites (we discuss this article in Sec. 7).

We checked Epic's claim on July 5, 2022 and found that none of the MyChart sites in our dataset used Facebook Pixel, and 21% removed Google Analytics, confirming Epic's reported findings.

5.2 Telehealth Providers

5.2.1 Methodology

In Section 4, we identified PHI leaks on the back pages of four telehealth provider websites. We elected to notify all four of our findings. We contacted Amwell and MDLIVE via their web-based contact forms and we contacted PlushCare and Sesame Care using their "contact us" page email addresses. Excluding changing "MyChart" to "telehealth", the notification letter we sent to the telehealth providers was identical to the one we sent to the MyChart portals (Appdx. A). Where applicable, we also included the snippet of text regarding privacy policies mentioned in Section 5.1.2. The monitoring we performed of the telehealth providers was identical in timing to the MyChart portals in the previous section, with the exception of vendor (Epic) notification, as each telehealth provider is its own vendor.

5.2.2 Results

Unfortunately, we received no responses from *any* of the telehealth providers. We saw no change in the numbers reported for Table 4, even after our notification. In the time between our last measurement, July 5th, 2022, and the time of writing, Sesame Health added the Tiktok Analytics tracker to their telehealth site, leaking PHI to an additional third party social media tracker.

6 Discussion

There is a disconnect between HIPAA and the emerging online healthcare environment. In order to protect patients' privacy, it may be necessary to make changes to HIPAA, online healthcare systems, and third party policies regarding the collection and use of PHI.

6.1 Regulatory Guidance

The choice of which guidance should be issued to healthcare providers depends on how strictly one interprets HIPAA. We advocate for a stricter standard that we believe aligns with the current HIPAA rules, namely that **there should be no third-party resources on healthcare providers' websites**, including external JavaScript, images, or stylesheets, unless the third parties have a Business Associate Agreement with the healthcare provider. This suggestion is motivated by two insights:

(1) Just *loading* a third party resource can leak PHI unless the page and browser enforce a policy omitting the `Referer` header from third party requests.
(2) A third party resource may be changed by the third party any time it is requested. Third party resources may *begin* to leak PHI independent of healthcare provider action and awareness.

HIPAA allows for the disclosure of PHI to third parties via Business Associate Agreements (BAAs). BAAs prevent third parties from using PHI in a manner that violates patients' privacy. Some services used by MyChart and telehealth websites, like Callrail and Piwik, have instructions on how to sign BAAs with healthcare providers—Facebook and Google do not. Unless third party services have a BAA, their inclusion on healthcare websites runs the risk of the HIPAA violations demonstrated in Sections 3 and 4.

Alternatively, HIPAA could be updated with explicit policies for the design and use of third party web resources. This would help ensure patients' privacy while allowing third party resources to be used without the need for BAAs.

6.2 Advertising

Section 5.1.3 found healthcare providers use third party trackers for marketing. However, third parties *may* also be using this information. To better understand whether the leaked PHI *could* be used for advertising purposes, we validated whether this information was present in Google Takeout [49] and Facebook's user information [9]. These services provide users with the information Google and Facebook have collected about them.

We used a fresh Chrome browser install to sign up for Google and Facebook accounts. We ensured identifying cookies were installed into the browser. We then visited EHR portals and telehealth websites and leaked health information. After this, we waited for three days before checking Google and Facebook's information insight services. Browsing information related to patient portals and telehealth websites appeared for both Google and Facebook.

reCAPTCHA. We performed the experiment above for sites that loaded only Google's reCAPTCHA and no other third party trackers. We found that after three days Google Takeout did not mention any of the sites we visited that had reCAPTCHA enabled. It does not appear that user-associated reCAPTCHA data is recorded by Google.

We note, however, that reCAPTCHA sends unique identifier cookies to `google.com` (Sec. 3.6.4) and reveals *the fact* of treatment (logging in to a healthcare portal) to Google. Under current regulations, the inclusion of reCAPTCHA on the healthcare portals identified in Section 3 constitutes a HIPAA violation.

Privacy Policies. Google's Ad Personalization policy states medical ads are not conditioned on (1) long-term medical conditions, (2) products and services to treat long-term conditions, (3) health issues related to "intimate" body parts (genitals, bowels), (4) invasive procedures (including cosmetic surgery), or (5) disabilities [15]. This listing does not necessarily exclude information leaked by

EHR portals and telehealth sites. At the time of writing Facebook's privacy policy does not mention use of medical information [13].

6.3 Identified and Identifiable

This paper *does not* claim that collected PHI is *identified* by third parties like Google and Facebook, but does state the fact that the collected PHI is *identifiable*. The third parties collecting the PHI *could* choose to match the collected health information to a user account associated with the user's identity. This fact, the possibility of identification, makes the discovered PHI leaks a violation of HIPAA. Whether the third parties choose to perform this matching is not relevant to this paper.

7 Related Work

Third-party Web Tracking. Roesner et al. [44], and Mayer and Mitchell [39] were among the first to investigate web trackers' prevalence and behavior. Krishnamurty and Wills [33, 34] were also some of the first to identify third party information leaks in URL information (the referrer header) of HTTP requests. The next year, Krishnamurty et al. [32] noted the growing lack of defenses for information leaks in third party requests. Jang et al. [31] also provided an early empirical study of privacy violations by JavaScript web applications. Several PHI breaching trackers we examined match Bujlow et al.'s survey of current web tracking mechanisms, implementations, and defenses [22]. For example, Google Analytics tracked patients both by cookies and by interactions (e.g. button clicks).

Privacy Policies. Libert et al. [38] investigated the privacy policies of over 200,000 websites, checking for disclosure of third-party trackers' information collection. Amos et al. [19] studied longitudinal changes to privacy policies on a million websites. Neither of these works focuses on healthcare systems. Sunyaev et al. surveyed the availability and quality of mobile health app privacy policies [47]. In contrast, the current work measures the quality and change over time of healthcare website privacy policies. Sanchez et al. [45] found only 4% of 2,000 high-traffic websites provided a clear consent request for cookies, while only 2.5% actually removed cookies if users chose to opt-out of tracking. We found similar behaviors among EHR portals: none asked for consent to use third-party cookies.

Tracking on Health Related Websites. Ernie [50] is a browser extension to monitor trackers on health-related websites. The current work complements this work by studying patient health portals and PHI breaches due to third party trackers. Libert et al. [37] crawled 80,000 health-related websites by querying diseases using Bing and used WebXray to analyze these sites' web traffic. However, they did not analyze what type of information was sent by these trackers, nor did they analyze interactive tracking, e.g. HTTP requests triggered by button clicks. Downing et al. [25] examine browsing data exchanges between companies offering services for the Cancer community and Facebook for advertising purposes. This analysis was limited to Facebook trackers and did not measure PHI breaches or online healthcare systems. Zheutlin et al. [51] also considered tracking on websites related to health but did not consider healthcare provider systems.

A contemporary article by Feathers et al. in *The Markup* reported similar findings for Facebook Pixel as the present work [28]. Our analysis focused on a broader, deeper, and more rigorous measurement of third party services on patient portals by including services other than Facebook Pixel. Additionally, Feathers et al. studied the primary websites of the top 100 hospitals in the U.S. and do not focus, in particular, on patient health portals or telehealth websites. The publishing time of the article (June 15, 2022) was after our experiments (February 25, 2022). The article's popularity may have boosted the effects of our Epic notification (Sec. 5.1.4), further demonstrating the positive impact of vendor notification and communication of scientific discoveries on prevention PHI leaks.

HIPAA Compliance. Baker et al. [21] was one of the first to report on the importance of maintaining the laboratory test result privacy during electronic reporting under HIPAA. Later, Carrión et al. [23] presented a study of the privacy policies on 22 websites that stored patients' personal health records, and checked whether the privacy of patients' data was preserved under HIPAA guidelines. Garg et al. [29] presented reduce to automatically check HIPAA compliance in system audit logs. More recently, Vargas et al. [48] analyzed the HIPAA compliance of internet-connected medical devices in a major, multi-campus healthcare system. This paper differs from these prior studies in that it considers PHI breaches created by third-party trackers in web applications rather than information storage or embedded systems.

8 Conclusion

In this work we studied the prevalence of Protected Health Information (PHI) breaches in online healthcare systems by third party trackers. We found users' health information can be correlated to identifiers like name and email via HTTP cookies and developed methods for identifying online healthcare system features that leak PHI. Using this information, we conducted a large scale survey of 459 patient portal websites and 4 telehealth websites in U.S., finding a majority of websites contained at least one third party tracking tool and many leak the *fact* of treatment and patient identifiers to third parties.

We were able to identify specific website features disclosing personal and medical information to third parties, and discovered significant PHI breaches as a result of Google and Facebook trackers, including leaks of lab test results, phone numbers, and addresses. The websites affected service hundreds of thousands to millions of monthly visitors. Moreover, we performed a longitudinal study of tracking behaviors in online health services after notifying them of PHI breaches. In the following two months we found only 15.7% of notified providers removed third party trackers.

After notifying the Epic vendor about our discovered MyChart patient portal PHI leaks, we received a prompt response and observed extensive mitigation across providers, suggesting vendor notification is an effective intervention against PHI disclosures.

Acknowledgments

We thank Rucha Shastri and Rummana Alam from the University of Illinois College of Law for helping us understand the legal dimension of HIPAA. This research was supported by NSF award 1903612.

References

[1] 2013. Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification.

[2] 2019. Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default. https://blog.mozilla.org/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/.

[3] 2020. Full Third-Party Cookie Blocking and More. https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/.

[4] 2020. Google Analytics Click Tracking: Complete Guide. https://diib.com/learn/google-analytics-click-tracking/.

[5] 2020. SameSite Cookies Explained. https://web.dev/samesite-cookies-explained/.

[6] 2021. 100 of the Largest Hospitals and Health Systems in America. https://www.beckershospitalreview.com/100-of-the-largest-hospitals-and-health-systems-in-america-2021.html.

[7] 2021. What is Telehealth? https://www.telehealth.com/what-is-telehealth/.

[8] 2022. 10 of the Best Telemedicine Companies for 2022. https://www.healthline.com/health/best-telemedicine-companies.

[9] 2022. Accessing and Downloading Your Facebook Information. https://www.facebook.com/help/contact/180237885820953.

[10] 2022. Automatic Configuration. https://developers.facebook.com/docs/meta-pixel/advanced.

[11] 2022. Google's Service Specific Terms. https://cloud.google.com/terms/service-terms.

[12] 2022. LinkedIn Cookie Table. https://www.linkedin.com/legal/l/cookie-table.

[13] 2022. Meta Privacy Policy. https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0.

[14] 2022. MyChart. https://www.mychart.com/.

[15] 2022. Personalized Advertising. https://support.google.com/adspolicy/answer/143465?hl=en&ref_topic=7012636.

[16] 2022. Privacy Policy of the Children's Wisconsin App. https://childrenswi.org/about/privacy-practices/childrens-wi-app-privacy-policy.

[17] 2022. What is Considered Protected Health Information Under HIPAA? https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

[18] Katie Adams. 2021. 7 Stats that Show How Americans Used Telehealth in 2021. https://www.beckershospitalreview.com/telehealth/7-stats-that-show-how-americans-used-telehealth-in-2021.html.

[19] Ryan Amos, Gunes Acar, Elena Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. 2021. Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset. In *Proceedings of the Web Conference 2021*. 2165–2176.

[20] George J Annas. 2003. HIPAA Regulations: A New Era of Medical-Record Privacy? *New England Journal of Medicine* 348 (2003), 1486.

[21] Dixie B Baker. 2006. Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety. In *22nd Annual Computer Security Applications Conference (ACSAC'06)*. IEEE, 3–22.

[22] Tomasz Bujlow, Valentín Carela-Español, Josep Sole-Pareta, and Pere Barlet-Ros. 2017. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proc. IEEE* 105, 8 (2017), 1476–1510.

[23] Inma Carrión, Jose L Fernández-Alemán, and Ambrosio Toval. 2011. Usable Privacy and Security in Personal Health Records. In *IFIP Conference on Human-Computer Interaction*. Springer, 36–43.

[24] Tate Coray and Warburton Paul. 2021. Hospital Market Share. https://klasresearch.com/report/us-hospital-market-share-2021-emr-purchasing-continued-despite-covid-19/1839.

[25] Andrea Downing and Eric Perakslis. 2022. Health Advertising on Facebook: Privacy & Policy Considerations. *arXiv preprint arXiv:2201.07263* (2022).

[26] Steven Englehardt and Arvind Narayanan. 2016. Online Tracking: A 1-Million-Site Measurement and Analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1388–1401.

[27] Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W Felten. 2015. Cookies that give you away: The surveillance implications of web tracking. In *Proceedings of the 24th International Conference on World Wide Web*. 289–299.

[28] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu. 2022. Facebook Is Receiving Sensitive Medical Information from Hospital Websites. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[29] Deepak Garg, Limin Jia, and Anupam Datta. 2011. Policy Auditing Over Incomplete Logs: Theory, Implementation and Applications. In *Proceedings of the 18th ACM conference on Computer and communications security*. 151–162.

[30] Becker's Healthcare. 2021. EHR Market Share 2021: 10 Things to Know about Major Players Epic, Cerner, Meditech, and Allscripts. https://www.beckershospitalreview.com/ehrs/cerner-slips-2nd-year-but-holds-dominance-alongside-epic-for-ehr-market-share.html.

[31] Dongseok Jang, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. 2010. An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications. In *Proceedings of the 17th ACM conference on Computer and communications security*. 270–283.

[32] Balachander Krishnamurthy, Konstantin Naryshkin, and Craig Wills. 2011. Privacy leakage vs. protection measures: the growing disconnect. In *Proceedings of the Web*, Vol. 2. 1–10.

[33] Balachander Krishnamurthy and Craig Wills. 2009. Privacy Diffusion on the Web: a Longitudinal Perspective. In *Proceedings of the 18th international conference on World wide web*. 541–550.

[34] Balachander Krishnamurthy and Craig E Wills. 2009. On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM workshop on Online social networks*. 7–12.

[35] Dimi Lee and Christoph Kerschbaumer. 2021. Firefox 87 Trims HTTP Referrers by Default to Protect User Privacy. https://blog.mozilla.org/security/2021/03/22/firefox-87-trims-http-referrers-by-default-to-protect-user-privacy/.

[36] Tai-Ching Li, Huy Hang, Michalis Faloutsos, and Petros Efstathopoulos. 2015. Trackadvisor: Taking Back Browsing Privacy from Third-Party Trackers. In *International Conference on Passive and Active Network Measurement*. Springer, 277–289.

[37] Timothy Libert. 2015. Privacy implications of health information seeking on the web. *Commun. ACM* 58, 3 (2015), 68–77.

[38] Timothy Libert. 2018. An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. In *Proceedings of the 2018 World Wide Web Conference*. 207–216.

[39] Jonathan R Mayer and John C Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *IEEE symposium on security and privacy*. IEEE, 413–427.

[40] Maud Nalpas. 2020. A New Default Referrer-Policy for Chrome - strict-origin-when-cross-origin. https://developer.chrome.com/blog/referrer-policy-new-chrome-default/.

[41] U.S. News. 2022. Best Hospitals Honor Roll. https://health.usnews.com/best-hospitals/rankings.

[42] The Office of the National Coordinator for Health Information Technology (ONC). 2017. Health Care Professional Health IT Developers. https://www.healthit.gov/data/quickstats/health-care-professional-health-it-developers.

[43] The Office of the National Coordinator for Health Information Technology (ONC). 2020. Individuals' Access and Use of Patient Portals and Smartphone Health Apps. https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020.

[44] Franziska Roesner, Tadayoshi Kohno, and David Wetherall. 2012. Detecting and Defending Against {Third-Party} Tracking on the Web. In *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*. 155–168.

[45] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proceedings of the 2019 ACM Asia conference on computer and communications security*. 340–351.

[46] Sebastian Schelter and Jérôme Kunegis. 2016. Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers. In *Tenth International AAAI Conference on Web and Social Media*.

[47] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. 2015. Availability and Quality of Mobile Health App Privacy Policies. *Journal of the American Medical Informatics Association* 22, e1 (2015), e28–e33.

[48] Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin RB Butler, and Patrick Traynor. 2019. Digital Healthcare-Associated Infection: A Case Study on the Security of a Major Multi-Campus Hospital System.. In *NDSS*.

[49] Web Webster. 2021. Google Takeout: Why You Need It and How to Use It. https://www.lifewire.com/what-is-google-takeout-4173795.

[50] Vera Wesselkamp, Imane Fouad, Cristiana Santos, Yanis Boussad, Nataliia Bielova, and Arnaud Legout. 2021. In-Depth Technical and Legal Analysis of Tracking on Health Related Websites with ERNIE Extension. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. 151–166.

[51] Alexander R Zheutlin, Joshua D Niforatos, and Jeremy B Sussman. 2022. Data-Tracking on Government, Non-Profit, and Commercial Health-Related Websites. *Journal of general internal medicine* 37, 5 (2022), 1315–1317.

A Notification Letter Template

The following notification letter was sent to providers that had both Google Analytics and Facebook Pixel on front and back pages of their MyChart portal. For websites with different trackers, we will modify the trackers listed in the letter accordingly.

> Dear *(Provider name)* Administrator,
> I am *(PI title and affiliation)*. My research team is studying information leaks to third parties on Web sites that display individual health information. We want to inform you that your organization's MyChart Patient Portal uses Google Analytics and Facebook Pixel to track visitors to your Web site. These trackers send the following information to Google and Facebook about the individuals viewing your site:
> 1. Personal Information, such as name, address, phone number, email, gender, and birthday (sent by Facebook Pixel).
> 2. Medications (sent by Facebook Pixel).
> 3. Plans of care, including upcoming lab tests (sent by Facebook Pixel).
> 4. Information about appointments, including dates, hospitals, and topics (sent by Facebook Pixel).
> 5. URLs and titles of the pages they visit, which include the topics of the pages (sent by Google Analytics, Facebook Pixel).
>
> This happens when a user accesses your Web site and views different services, or clicks on the contents and buttons in Web forms, such as the forms on the pages of "Personal Information", "Medications", "Plan of Care", and "Schedule an Appointment". While we did not specifically verify that your Web site also sends test results to Facebook, based on your site configuration, we believe that this information would also be sent.
> In addition to the information relating to medical treatment above, a user's Web browser sends Web cookies to Google, which allow Google to identify visitors to your Web site. For visitors who are logged in to Google, the cookie is associated with their Google account, which includes their name and email address. This makes the health information transmitted to Google identifiable.
> When we accessed your MyChart Web site, we were not asked for consent to share health information with Google and Facebook, nor did your Web site provide any indication that the information above is being sent to these companies.
> When we accessed your MyChart Web site, we were not asked for consent to share health information with Google, nor did your Web site provide any indication that the information above is being sent to Google.
> Sincerely, *(PI name and contact information)*

The last paragraph was only included if the provider did not have a privacy policy or a privacy policy that did not mention third-party trackers. If we did not confirm that Google Analytics was present on the back pages, the sentence "The Google Analytics tracker sends the following information to Google about the individuals viewing your site" in the first paragraph was replaced by "While we could not verify that the same tracker is present on your Web site after logging in, we have found that this is usually the case based on our analysis of other MyChart Web sites. If present on your MyChart site after logging in, Google Analytics would send the following health information to Google about the individuals viewing your site."

B MyChart Websites Under Notification

We divide the websites into several categories based on the trackers we found and whether we could create accounts to confirm their tracking behaviors. The following hospitals use both Facebook Pixel and Google Analytics on patient record pages. These represent the most severe case of information disclosure to third parties. Note that four of them are confirmed and the last one is unconfirmed. The data for the *Tracker* column is collected on December 14, 2021, and for the *After notify* column is collected on February 25, 2022.

No.	Name	Website	Tracker	Confirm	After notify
1	Community Health Network	mychart.ecommunity.com/MyChart	FP, GA	Y	FP, GA
2	FastMed	mychart.fastmed.com/MyChart	FP, GA	Y	GA
3	Premier Health	mychart.premierhealthpartners.org/mychart	FP, GA	Y	FP, GA
4	Edward-Elmhurst Health	mychart.eehealth.org/mychart/	FP, GA	Y	GA
5	Beaver Medical Group	www.mybeaverchart.com/MyChart	FP, GA	N	GA

The following hospitals use Google Analytics on patient record pages and is confirmed by us:

No.	Name	Website	tracker	confirm	removed
6	UC Health	mychart.uchealth.org/MyChart	GA	Y	Y
7	Lehigh Valley	Health Network, www.mylvhn.org/MyChart	GA	Y	
8	OSF HealthCare	www.osfmychart.org/osfmychart	GA	Y	
9	SSM Health	mychart.ssmhc.com/mychart	GA	Y	
10	Kettering Health	mychart.ketteringhealth.org/MyChartPRD	GA	Y	
11	Spectrum Health	mychart.spectrumhealth.org/MyChart	GA	Y	
12	Ochsner Health	my.ochsner.org/PRD	GA	Y	
13	Advocate Aurora Health	livewell.aah.org/Chart	GA	Y	

The following Hospitals use Google Analytics on their MyChart front page. We could not confirm whether Google Analytics trackers were present after logging in because we could not create an account on these sites.

No.	Name	Website	tracker	confirm	removed
14	Memorial Healthcare System	mychart.mhs.net/mychart	GA	N	Y
15	Community Care Plan	mychart.mhs.net/mychartCCP	GA	N	Y
16	AUB Medical Center	myaubhealth.aubmc.org.lb/mychartprd	GA	N	Y
17	Salem Health	mychart.salemhealth.org/mychart	GA	N	Y
18	Amita Health	mychart.presencehealth.org/mychart	GA	N	Y
19	Yale health	mychart.ynhhs.org/MyChart-PRD	GA	N	Y
20	Children's Wisconsin	mychart.chw.org/mychart	GA	N	Y
21	Rush University Medical Center	mychart.rush.edu/MyChart	GA	N	
22	UC Davis Health	mychart.ucdavis.edu/MyChart	GA	N	
23	UChicago Medicine	mychart.uchospitals.edu/mychart	GA	N	
24	Sarasota Memorial Health Care System	ohnmychart.org/smh	GA	N	
25	Middlesex Health	mychart.middlesexhealth.org/mychart	GA	N	
26	OrthoVirginia	mychart.orthovirginia.com/MyChart	GA	N	
27	McFarland Clinic	mychartiowa.com/mychartprd	GA	N	
28	UT Physicians	myuthealth.org/MyChart	GA	N	
29	St. Luke's Health	mychart.slhs.org/mychart	GA	N	
30	University of Kansas Health System	mychart.kansashealthsystem.com/MyChart	GA	N	
31	Houston Methodist	mychart.houstonmethodist.org/mychart-prod	GA	N	
32	Prevea Health	myprevea.com/MyPrevea	GA	N	
33	Peace Health	my.peacehealth.org/MyPeaceHealth	GA	N	
34	Mercy Medical Center (Baltimore)	mychart.mdmercy.com/mychartv	GA	N	
35	Barton Healthcare System	mychart.bartonhealth.org/mychart	GA	N	
36	Grady Health System	mychart.gradyhealth.org/mychart	GA	N	
37	Honor Health	mychart.honorhealth.com/mychart	GA	N	
38	DuPage Medical Group	mychart.dupagemedicalgroup.com/mychart	GA	N	
39	Jefferson Health	mychart.jefferson.edu/mychart	GA	N	
40	MultiCare Health System	mychart.multicare.org/mymulticare	GA	N	
41	Rochester Regional Health	mycare.rochesterregional.org/mychart	GA	N	
42	Renown health	mychart.renown.org/mychart	GA	N	
43	Texas Health Resources	mychart.texashealth.org/MyChart	GA	N	
44	Cone Health	mychart.conehealth.com/MyChart	GA	N	
45	Bon Secours Mercy Health	mychart.mybonsecours.com/mychart	GA	N	
46	Catholic Health	mychart.chsli.org/mychartprod	GA	N	
47	St. Tammany Health System	mychart.stph.org/mychartstph	GA	N	
48	Riverside Health System	riversidemychart.org/MyChart-PRD	GA	N	
49	Marshall Medical Center	mychart.marshallmedical.org/MyChart	GA	N	
50	BronxDocs	my.bronxdocs.com/MyChartBD	GA	N	
51	Optum Care	epicmychart.optum.com/mychart	GA	N	
52	Sparrow Health Systems	mychart.sparrow.org/mychart	GA	N	
53	Chesapeake Regional Healthcare	mychart.chesapeakeregional.com/MyChart	GA	N	
54	Penn Medicine	secure.mypennmedicine.org/MyPennMedicine	GA	N	
55	Wexner Medical Center	mychart.osu.edu/osumc	GA	N	
56	Beaumont Health System	mybeaumontchart.com/mychart	GA	N	
57	Baptist Healthcare	mychart.baptisthealth.com/mychart	GA	N	
58	Central Vermont Medical Center	mychart.cvmchospital.org/mychart	GA	N	
59	Covenant Health	mychart.covenanthealth.net/MyChart	GA	N	
60	Terrebonne General Health System	ohnmychart.org/TGMC	GA	N	
61	Bellin Health	mybellin.org/MyChart	GA	N	
62	Kelsey-Seybold Clinic	mykelseyonline.com/MyChart	GA	N	
63	Duke University Health System	dukemychart.org/home	GA	N	
64	Loyola Medicine	myloyola.luhs.org/mychart	GA	N	
65	Mercer Health	mychart.osu.edu/mercerhealth	GA	N	
66	Legacy Health	myhealth.lhs.org/MyHealth	GA	N	