feroot

Feroot Client-Side Security Investigation Report

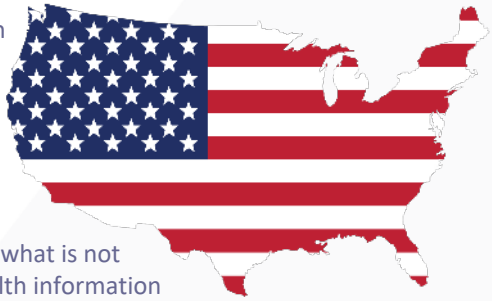
# Beware of Pixels & Trackers: Healthcare Websites Are Hemorrhaging Patient Information

November 2, 2023

# Introduction

## Background

The healthcare industry massively adopted use of web tracking tools such as pixels and trackers on healthcare websites and portals as part of the growth strategy. These tracking tools, including Google Analytics and Meta Pixel are developed and maintained by third-party vendors, collect user data to analyze user interactions with websites, patient care portals, and/or for online marketing.



While it's common practice for companies to use pixel and tracking tools what is not widely known is how common it is and to if or what personal/private health information is being transferred to various actors, without explicit and Informed patient and/or user consent. Thus many instances of healthcare organizations exposing PHI (Protected Health Information) to third-party vendors of pixel and tracking tools became known in 2022 and 2023. For example, on August 17, 2023 Advocate Aurora Health proposed a $12.25 million settlement to resolve a consolidated class action lawsuit filed over the impermissible disclosure of patient data, between October 24, 2017, and October 22, 2022, via web tracking operated by Google and Facebook and various other third-party vendors.

**Assessment scope:**

**33,408**
unique healthcare webpages

**1,515**
on unique healthcare websites

**530**
healthcare providers

## Purpose

We conducted this research to determine the level of potential exposure of ePHI to web tracking and various other third-party tools used by healthcare providers on their websites. Additionally, the research was aimed to establish the probable likelihood of compliance incidents, security incidents and breaches originating from the use of web tracking tools as defined below:

- **Compliance incident:** is an occurrence or a set of circumstances where an organization fails to adhere to or violates applicable laws, regulations, policies, or standards.
- **Security Incident** is a security event that jeopardizes the integrity, confidentiality, or availability of information assets.
- **Security Breach:** is a type of incident where there is confirmed disclosure, not a potential exposure, of data to an unauthorized entity.

## Scope

This research examined over **530** organizations with unique websites, **1,515** websites and **33,408** webpages were analyzed in depth. The examined websites included hospitals, state and federal healthcare sites and health insurance companies.

# Introduction

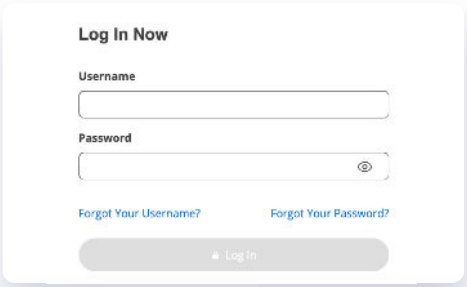
## Web Tracking Tools in Healthcare

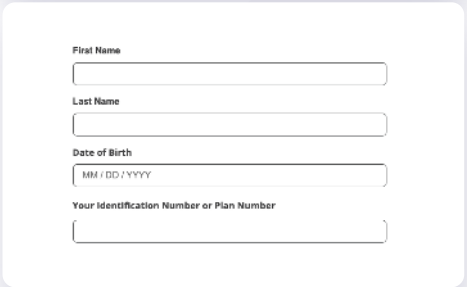
With the digitization of healthcare services, web tracking technologies and tools have become common and abundantly used by healthcare providers. These technologies and tools are used by healthcare organizations to enhance patient care, patient digital experience and to market online. Tracking tools gather, analyze, and store data about users' interactions with online platforms.

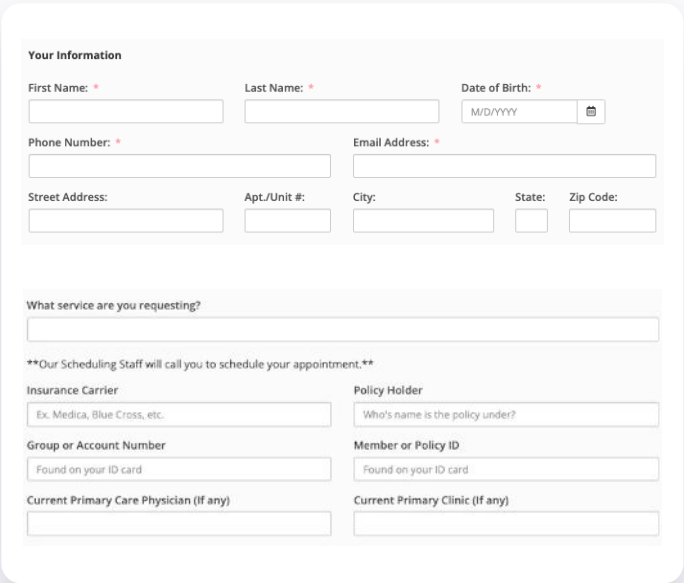
However, there are significant concerns about patient privacy, data security and compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and liabilities when handling protected health information (PHI). For instance, the presence of this tracker has led to class action lawsuits against hospitals like **Advocate Aurora, WakeMed** and many others in 2022 and 2023.

## Collection of Consumers' Health Information on Authentication (Login) and Registration webpages

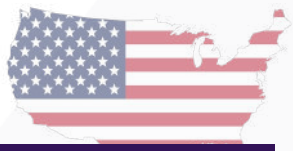
The use of tracking technologies on healthcare websites, while beneficial for growth and marketing analytics, it also introduces new vulnerabilities and weaknesses. The cost and the volume of data loss and compliance incidents, attributed to tracking technologies on authentication and registration webpages, is rising. These incidents now constitute a substantial portion of the overall data compromise events, underscoring the urgent need to address the risks associated with embedding such technologies on sensitive webpages.



# Executive Summary



## What Data Assets Are at Stake

**Protected Health Information (PHI):**
PHI includes any information that can be linked to a specific individual's health status, provision of healthcare, or payment for healthcare. Examples are names, addresses, birth dates, Social Security numbers, medical records, and more.

**Online Scheduling and Appointment Data:**
If this data includes identifiable information about a patient and their healthcare services, it would be considered PHI and thus needs to be HIPAA-compliant.

**Search Queries:**
If users' search queries for specific health-related information on a healthcare provider's website could be considered PHI if they be linked back to an individual.

## Top 3 Exposure Vectors

**Exposure Vector 1 - Tracking on User-Authenticated Webpages.**
Tracking technologies on user-authenticated webpages, such as patient portals, can access PHI, including diagnosis, treatment information and appointment details.
**Finding:**
Web trackers are accessing and reading user inputs on **14.9%** of all Authentication (Login) and Registration forms. This indicates ongoing partial or complete disclosure of consumer information to these web tracking technologies.
**73.2%** of Authentication (Login) and Registration pages load web trackers, granting them full access to user inputs, leading to around 3 out of 4 pages potentially exposing consumer information to web tracking technologies.

**Exposure Vector 2 - Tracking on Unauthenticated Webpages.**
Tracking technologies can access PHI on webpages that don't require users to login.
**Finding:**
**86.2%** of healthcare websites load tracking technologies on pages discussing specific symptoms or conditions, or allowing appointment scheduling, potentially disclosing individuals' email, IP address, and other data.

**Exposure Vector 3 - Use of Vulnerable and Outdated JavaScript Libraries.**
Using vulnerable libraries like jQuery exposes healthcare websites providers to significant risks, including potential breaches or unauthorized access to PHI
**Finding:**
**91%** of websites use jQuery libraries. **45%** of which have vulnerabilities and **14%** are over a decade old.

**Findings:**

**86.2%**
of websites use web trackers that collect and transfer user data.

**14.9%**
of all Authentication (Login) and Registration webpages have trackers that are reading what consumers are typing into account name and passwords forms.

**73.2%**
of all Authentication (Login) and Registration webpages use behind-the-scenes tracking technologies.

**45.8%**
of all detected jQuery libraries possess known vulnerabilities. 14% of jQuery libraries are more than 10 years old.

# Risks

## Top 5 Risks to Healthcare Providers

Impermissible Disclosures of PHI via online tracking technologies and other third-party tools can lead to unauthorized disclosures of Protected Health Information (PHI) to third-party vendors. Such disclosures can expose healthcare providers to the following business risks:

**Risk 1 - Legal and Regulatory Penalties:**
Healthcare providers can face significant legal and regulatory penalties for non-compliant use of Web Tracking tools. This includes actions from bodies like the HHS Office for Civil Rights (OCR) and the Federal Trade Commission (FTC).

**Risk 2 - Class Action Lawsuits:**
The presence of third-party trackers on healthcare websites can lead to class action lawsuits. Healthcare providers such as Advocate Aurora and WakeMed faced such lawsuits due to alleged unauthorized data collection by Meta's tracker.

**Risk 3 - Reputational Damage:**
Collection and loss of personal information by third-party tracking technologies on healthcare websites can erode trust among patients and the general public. This can potentially lead to a loss of patients and business.

**Risk 4 - Liabilities due to Third-Party Entity Data Breaches:**
Healthcare providers may be liable under HIPAA and some state level privacy laws when a Third Party Entity improperly discloses ePHI. The use of third-party tracking technologies increases the likelihood of healthcare providers being exposed to potential data breach incidents should a third-party vendor suffer a security breach and sensitive patient data collected through tracking technologies is compromised.

**Risk 5 - Legal Repercussions from State-Level Privacy Laws:**
State law can give patients the right to bring a civil suit against a business for actual damages in some cases of violation of state laws on health information privacy. Therefore healthcare providers should be aware of possible risks posed by applicable state privacy laws in addition to federal regulations, as violations of state-specific privacy laws can lead to additional legal actions, penalties and lawsuits from patients or other entities.

**Findings:**

**12**

Average number of web trackers on websites that use them.

**9.4**

Average number of web trackers per Authentication page (such as Login and Registration webpages) with access to user input fields, on webpages utilizing trackers.

**45.8%**

of all detected jQuery libraries possess known vulnerabilities, and 14% of jQuery libraries are over a decade old.

# Risks

## Top 3 Risks to Patients

Patients can face risks due to impermissible disclosures of PHI via online tracking technologies and other third-party tools:

**Risk 1 - Identity Theft and Fraud:**
Unauthorized access to PHI can provide cybercriminals with enough personal information to commit identity theft. With detailed health records, malicious actors can impersonate patients, potentially leading to fraudulent medical claims, acquiring medications illicitly, or other forms of medical identity fraud.

**Risk 2 - Loss of Confidentiality, Privacy and Personal Security:**
Loss of patient's sensitive health information, such as diagnoses, treatments, o medical histories can lead to stigmatization, personal embarrassments, discrimination, especially if the disclosed information pertains to mental healt issues, genetic disorders, or other sensitive conditions.

**Risk 3 - Financial Losses:**
Unauthorized access to PHI can also expose billing information, insurance details, and other financial data. This can lead to unauthorized transactions, false insurance claims, or other financial frauds, burdening patients with unwarranted financial liabilities.

**Findings:**

**80%**
of Login and Registration Pages have Input-Reading Third-Party Scripts and Libraries.

**86%**
of Login and Registration pages utilize third-party scripts and libraries.

**56**
Average Number of Data Transfers from Authentication Pages (such as Login and Registration)

# Findings

## Summary of Findings

Welcome to snapshot of our dive into the world of web tracking technologies in healthcare and telehealth sectors. We rolled up our sleeves and examined over a thousand websites and over 35,000 webpages, scrutinizing everything from login pages to specific medical condition discussions. The data table below lays out overview of key findings. In the pages below, you'll see the details — such as which sites are using tracking tools, how many have forms patients/users can fill out, and if forms are exposed to risks or could be in a middle of an incident. We also looked at what kind of data is being collected the most, if there are trackers and scripts on login and registration pages, any data being transferred, presence of vendors and threat intelligence across the supply chain. Enjoy!

| Description of Findings | Results |
|---|---|
| Total number of examined Healthcare & Telehealth organizations | 530 |
| Total number of websites examined | 1,515 |
| Total number of unique webpages examined | 33,408 |
| Total number of unique websites with web tracking tools | 1,307 |
| Percentage of websites with web tracking tools | 86% |
| Average number of Tracking tools (pixels, beacons, trackers, etc.) per website with tracking tools | 12 |
| Percentage of websites with any user-fillable forms | 97.4% |
| Number of Login and Registration pages found during the study | 8,299 |
| Number of websites with Login and or Registration pages | 1,271 |
| Percentage of Websites with Login and Registration Pages | 83.9% |
| Average Number of Login and or Registration pages per website for websites with Login and Registration pages | 6.5 |
| Number of Billing pages (payment forms) on unauthenticated webpages found during the study | 159 |
| Percentage of websites with Billing pages (payment forms) detected on unauthenticated webpages | 5.9% |
| Number of Webpages that mention special conditions or diagnosis | 2,241 |
| Percentage of websites with malicious hosts receiving data transfers or loading scripts into website | 1.1% |
| Total number of technology vendors found in the supply chain | 155 |
| Total number of tools from all the vendors. | 210 |
| Percentage of websites that use jQuery libraries | 91% |
| Percentage of jQuery libraries with known vulnerabilities | 45.8% |

Alphabet Google **95%** of websites have it

Meta facebook **60%** of websites have it

Microsoft **46%** of websites have it

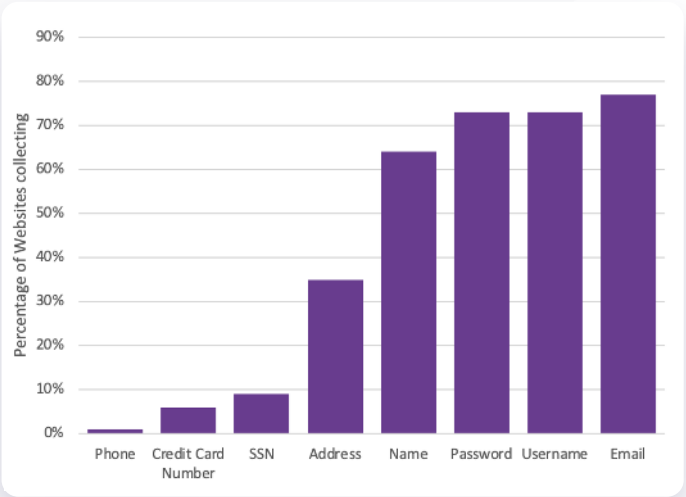
TikTok ByteDance **5%** of websites have it

jQuery **91%** of websites have it

# Findings

## Patient Information Collection on Unauthenticated Public Webpages

This section is focused on the most collected data assets and the percentage of websites that are gathering them. We're examining how the extensive collection of various data types is to help gauge potential risks and likelihood of risks. The graph below shows how extensive is the collection of user data entered by patients. The table below shows the associated likelihoods of data being collected. Taken together the risk of impermissible disclosures is real.




| Description | Percentage of Websites collecting it | Percentage of total data collected |
|---|---|---|
| **Email** | 77% | 30% |
| **Username** | 73% | 11% |
| **Password** | 73% | 11% |
| **Name** | 64% | 23% |
| **Phone** | 57% | 14% |
| **Address** | 35% | 8% |
| **SSN** | 9% | 2% |
| **Credit Card Number** | 6% | 1% |

# Findings

## Authentication (Login) and Registration webpages

Welcome to our section on Authentication (Login) and Registration webpages. We've examined the use of web tracking technologies, such as pixels, on healthcare websites. While these tools are beneficial for analytics, they introduce new risks, particularly on login and registration pages, where sensitive information is often entered.

| Description | Results |
|---|---|
| Number of websites with Login and/or Registration pages | 1,271 |
| Percentage of Websites with Login and Registration Pages | 83.9% |
| Average Number of Login and/or Registration pages per website for websites that have Login and/or Registration pages | 6.5 |
| Number of Login and Registration Pages | 8,299 |
| Number of all unique user fillable forms detected on all websites | 14,658 |
| Number of all user fillable forms detected on all websites | 55,216 |

## Vendors and Tracking Tools

The table presents the average presence of tracking technologies from various vendors on healthcare websites. It also provides insight to vendor management and compliance teams in ensuring secure, compliant use of these technologies and in managing Business Associate Agreements (BAAs) and Software Bills of Materials (SBOMs) effectively.

| Description | Results |
|---|---|
| Total number of unique vendors on all websites | 155 |
| Total number of tools from all the vendors | 210 |
| Percentage of Websites with any trackers (advertising, analytics, customer service, social media) | 86.3% |
| Average trackers per website for websites with trackers | 12 |
| Percentage of Login and Registration page with trackers having access to what users are typing into forms | 73.2% |
| Percentage of websites that have Login pages actively reading and processing what users are typing into forms | 14.9% |
| Percentage of Login pages with trackers doing active data reads for webpages with trackers | 15.6% |
| Percentage of all Login pages with trackers reading and processing what users are typing into forms | 11.4% |
| Percentage of Websites with Alphabet (Google) tracking tools | 95% |
| Percentage of Websites with Meta (Facebook) tracking tools | 60% |
| Percentage of Websites with Microsoft (Bing Ads, LinkedIn Ads) tracking tools | 46.3% |

# Findings

## Scripts and Libraries on Authentication, Registration and Public Pages

The table below illustrates the extent of JavaScript scripts and libraries presence across all webpages of the analyzed healthcare websites. While these elements are essential for website functionality and user experience, their quantity highlights potential concerns regarding vulnerabilities and the risk of compromised code.

These insights enable the Application Security team as well as the vendor management and compliance teams to managing Business Associate Agreements (BAAs) and Software Bills of Materials (SBOMs).

| Description of Findings | Results |
|---|---|
| Total number of scripts found on websites | 327,207 |
| Total number of third-party scripts found on websites | 152,570 |
| Percentage of third-party scripts in the software supply chain of websites | 47.0% |
| Percentage of Websites with any third-party scripts | 96.0% |
| Average number of third-party scripts per website for website has third-party scripts | 104 |
| Average Number of third-party scripts on Login and Registration Pages | 22 |
| Percentage of Login and Registration webpages with third-party scripts | 86.0% |
| Percentage of Login and Registration Pages with third-party scripts Reading Inputs | 80.0% |
| Percentage of Websites with Login and Registration Pages with third-party scripts Reading Inputs | 74.0% |
| Number of websites with HTML inline scripts | 1,506 |
| Percentage of websites with HTML inline scripts | 99.4% |
| Number of websites with eval scripts | 1,103 |
| Percentage of websites with eval scripts | 72.8% |

# Findings

## Data Transfers by Scripts, Web Trackers and Pixels

This section delves into our findings related to data transfers conducted by scripts, trackers, and pixels across various webpages. The insights provided here are primarily designed to assist Application Security teams, privacy compliance teams, and legal counsel in understanding and mitigating the risks associated with these data transfers, ensuring a secure and compliant online environment.

| Description of Findings | Results |
|---|---|
| Total number of data transfers | 2,093,302 |
| Average number of data transfers per website | 1,382 |
| Average number of data transfers per webpage | 63 |
| Number of Websites with libraries and/or transfers from/to Banned companies | 66 |
| Percentage of websites with tools loaded from and/or data transferred to companies banned by the federal and state executive orders. | 4.4% |
| Number of Websites with libraries and/or transfers from/to Russia | 6 |
| Percentage of Websites with libraries and/or transfers from/to Russia | 0.4% |

## Countries Receiving Tracking Data by Volume of Transfers

| | Country |
|---|---|
| 1 | USA |
| 2 | Canada |
| 3 | Ireland |
| 4 | Germany |
| 5 | Denmark |
| 6 | Singapore |
| 7 | France |
| 8 | United Kingdom |
| 9 | United Arab Emirates |
| 10 | Netherlands |
| 11 | Russia |
| 12 | Finland |
| 13 | Japan |

| | Country |
|---|---|
| 14 | India |
| 15 | Slovenia |
| 16 | Egypt |
| 17 | Mexico |
| 18 | Sweden |
| 19 | Argentina |
| 20 | Colombia |
| 21 | Australia |
| 22 | Ecuador |
| 23 | Brazil |
| 24 | Algeria |
| 25 | Belgium |
| 26 | Spain |

# Findings

## Vendors Supply Chain Threat Intelligence

This section is focused on Vendors Supply Chain Threat Intelligence. The following tables provide an overview of how many vendors and tools were found to be present in the software supply chain of healthcare websites, associated threats and vulnerabilities. The top 40 tracking tools present on healthcare websites, the percentage of websites for each tool and the corresponding percentage of data transfers. These finding help organizations in assessing potential exposure to security, privacy, and compliance risks, as well as calculating the probability percentage of these risks materializing.

| Description of Findings | Results |
|---|---|
| Total number of technology vendors found in the supply chain | 155 |
| Total number of tools from all the vendors. | 210 |
| Percentage of websites with tools loaded from and/or data transferred to companies banned by the federal and state executive orders. | 4.4% |
| Percentage of websites with malicious hosts receiving data transfers or loading scripts into website | 1.1% |
| Percentage of websites that use jQuery libraries | 90.9% |
| Number of versions of jQuery libraries detected | 64 |
| jQuery library versions older than 10 years | 14% |
| jQuery library with Vulnerabilities (Pre 3.5.0 version) | 45.8% |

## Threats

### Threat 1 - Impermissible Disclosures of PHI:

Disclosures of PHI to tracking technology vendors that without permission to disclose PHI and there is no BAA with the vendor.

### Threat 2 - Unauthorized Collection of PHI:

Where pixels, tracking tools and technology vendors collect PHI on websites and webpages.

### Threat 3 - China and Russia:

We found instances of patient data being collected by tracking tools controlled by companies under jurisdiction of China and Russia.

# Findings

## Vendors Supply Chain Threat Intelligence (continued)

This table highlights the top 40 tracking tools present on healthcare websites, the percentage of websites for each tool and the corresponding percentage of data transfers.

| | Company | Tools, such as web trackers, owned by the company | Percentage of websites that use company's tools | Percentage of Data Transfers by company |
|---|---|---|---|---|
| 1 | Alphabet | Google Remarketing, Google Tag Manager, Google Analytics, Google+, Google Analytics Audiences, Google AdWords | 95.03% | 33.11% |
| 2 | Meta | Facebook Business, Facebook Connect, Facebook Social Graph | 60.06% | 11.28% |
| 3 | Microsoft | LinkedIn Analytics, LinkedIn Widget, Bing Ads, LinkedIn Ads | 46.29% | 7.94% |
| 4 | AppNexus | AppNexus | 36.19% | 2.82% |
| 5 | Yahoo | Yahoo | 30.91% | 2.32% |
| 6 | Oracle | BlueKai, AddThis, Oracle Eloqua | 26.63% | 2.18% |
| 7 | Adobe | Adobe Audience Manager, Adobe Marketing Cloud, Omniture, Analytics | 26.09% | 4.08% |
| 8 | The Trade Desk | theTradeDesk | 21.27% | 1.70% |
| 9 | New Relic | New Relic | 19.74% | 1.11% |
| 10 | Telenor Group | Tapad | 19.20% | 1.53% |
| 11 | Acxiom | LiveRamp | 17.44% | 1.44% |
| 12 | Rubicon | Rubicon | 17.29% | 1.55% |
| 13 | PubMatic | PubMatic | 16.68% | 1.28% |
| 14 | OpenX | OpenX | 15.38% | 1.28% |
| 15 | Index Exchange | Index Exchange | 15.00% | 0.97% |
| 16 | Contentsquare | Clicktale, Hotjar | 14.69% | 1.50% |
| 17 | Nielsen | eXelate | 13.08% | 1.10% |
| 18 | Twitter | Twitter Ads, Twitter Syndication, Twitter Button, Twitter Analytics | 12.32% | 1.82% |
| 19 | Neustar | Aggregate Reach (Neustar) | 12.24% | 0.94% |
| 20 | TripleLift, Inc. | Triplelift | 11.94% | 0.98% |
| 21 | Live Ramp | Live Ramp | 11.86% | 0.87% |
| 22 | IPONWEB | IPONWEB | 9.87% | 0.64% |
| 23 | Crazy Egg | Crazy Egg | 9.26% | 0.77% |
| 24 | StackAdapt | StackAdapt | 8.88% | 0.68% |
| 25 | Nordic Capital | Siteimprove Analytics | 8.72% | 0.94% |
| 26 | Marketo | Marketo | 8.57% | 0.81% |
| 27 | Drawbridge | Drawbridge | 8.57% | 0.20% |
| 28 | Lytics | Lytics | 8.11% | 0.85% |
| 29 | SAP | Qualtrics, Gigya | 7.42% | 0.65% |
| 30 | HubSpot | Hubspot Livechat, Hubspot, Hubspot Forms | 7.04% | 1.15% |
| 31 | Teads | Teads | 6.20% | 0.47% |
| 32 | Taboola | Taboola | 6.12% | 0.49% |
| 33 | AdRoll | AdRoll | 5.43% | 0.47% |
| 34 | Automattic | Wordpress Stats, Gravatar | 5.20% | 0.35% |
| 35 | TikTok / ByteDance | TikTok | 4.90% | 0.46% |
| 36 | Medallia | Decibel Insight, Kampyle | 4.74% | 0.74% |
| 37 | Wistia | Wistia | 4.67% | 0.10% |
| 38 | LiveIntent | Live Intent | 4.59% | 0.19% |
| 39 | Outbrain | Outbrain | 4.21% | 0.31% |
| 40 | ExactTarget | Pardot | 3.83% | 0.36% |

# Recommendations

**Recommendation 1 - Establish and Maintain a Data Inventory:**

**Identify all Data Creation and Ingestion points on all websites and web portals.**
Begin by identifying all sources of data, including electronic health records (EHRs), patient portals, billing systems, and any other webpages where patient data is created and or ingested. Such as:

- Patient Registration/Sign-Up Pages where patients can input personal details such as name, date of birth, address, contact information, and sometimes preliminary medical history.
- Online Appointment Booking Systems where patients can schedule, reschedule, or cancel appointments and might provide reasons for the visit, preferred doctors, and preferred time slots, which become part of the patient's data.
- Health Record (EHR) Access Portals where patients can view, update, or add to their medical records.
- Billing and Payment Portals where patients can view their bills, make payments, dispute charges and/or receive payment assistance. These pages can require input of insurance details, credit card information, and other billing-related data.
- Telehealth Consultation form where patients might input symptoms, upload images or documents related to their condition, and have video consultations, all of which involve the creation or ingestion of patient data.

**Categorize Data.**
Once data sources are identified, categorize the data. This could be based on the type of data (e.g., personal details, medical history, billing information) or its sensitivity (e.g., public, confidential, restricted).

**Automate Data Asset Inventory Management.**
Consider using automated tools or software that can help in creating and maintaining the data inventory. These tools can periodically review and audit the data inventory, track data in real-time, provide alerts for discrepancies, and generate reports as needed. This helps in identifying any new data sources, ensuring that the inventory is up-to-date, and verifying that old or redundant data is appropriately managed.

**Document Data Flow.**
Understand and document how data flows to organization’s systems as well as third-parties. This can include how data is collected by, processed, stored, shared with third-party tracking technologies and vendors.

# Recommendations

## Recommendation 2 - Control Data Access on Webpages:

**Limit Data Sharing with Third-Party Vendors**
When integrating third-party tools or scripts, especially those related to marketing or analytics, configure them to share only the minimum necessary data. Explicitly define what data these tools can access and ensure they don't have permissions beyond their functional requirements.

- **Benefit:**

By limiting the scope of data access, healthcare organizations can ensure that third-party vendors don't inadvertently access or store sensitive patient information.

**Enable Access Controls on Form and Form field-level.**
Implement Security Policies to restrict JavaScript scripts and libraries from accessing unapproved content on webpages.

- **Benefit:**

This can prevent unauthorized scripts, pixels, or third-party tools from collecting PHI (Protected Health Information) such as Medical record numbers, home or email addresses, dates of appointments, Credential information on a login webpage and/or registration pages and web visitor information on webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage thereby minimizing potential data breaches.

**Implement Content Security Policy (CSP).**
Use a Content Security Policy to restrict the sources and types of content that can be executed on the website. This can prevent unauthorized scripts, pixels, or third-party tools from running without explicit permission.

- **Benefit:**

CSP acts as a security layer, ensuring that only approved content runs on the website to minimize potential data loss and data breaches.

# Recommendations

**Recommendation 3 - Establish and Maintain a Vulnerability Management for the Client-Side Runtime environment:**

**Shift-Left and Traditional Vulnerability Scanning are not Enough.**
While implementing routine vulnerability scanning using trusted tools and platforms, including both static (SAST) and dynamic (DAST) application security testing methods become a common practice, it's simply not enough. The traditional approach is focused on catching vulnerabilities in the development process, it overlooks the dynamic and evolving nature of threats that emerge in the post-deployment.

Note: this is where the concept of **"Shift Right"** becomes crucial for healthcare, where webpages and websites utilize pixels and tracking technologies. Shifting right emphasizes the vital importance of focusing on the post-implementation stages when tracking tools are loaded into the user experience in real time. Given the ever-evolving and constantly improving web healthcare platforms, vulnerabilities related to third-party providers, tools and tracking technologies can emerge after they are integrated.

With the dynamic nature of healthcare webpages and the continuously changing risks associated with pixels and trackers, it's imperative to persistently monitor, assess, and address potential threats in live and real time settings.

- **Benefit:**

By adopting Shift Right practices, healthcare organizations can ensure they're not only identifying risks early on but are also prepared to tackle and mitigate threats that arise in real-time, preventing unintended data sharing and loss.

# Recommendations

**Recommendation 4 - Establish and Maintain BAA management processes for Third-party Providers in Your Digital Supply Chain of Websites and Webpages:**

**Identify and Inventorize Third-Party Tools and their Providers.**
Before establishing BAAs, initiate a comprehensive discovery process to identify all third-party tracking tools and technologies loaded on healthcare websites and webpages. This will provide a clear understanding of which tools might be accessing or processing PHI.

- **Benefit:**

By identifying all third-party integrations, healthcare organizations can ensure that no tool is overlooked, ensuring comprehensive coverage and compliance.

**Ensure Proper Disclosures.**
Once all tools are identified, ensure that any disclosures of Protected Health Information (PHI) to these third-party vendors are specifically permitted by the Privacy Rule. Only disclose the minimum necessary PHI to achieve the intended purpose.

- **Benefit:**

Proper disclosures ensure that patient data is shared in a controlled and compliant manner, reducing the risk of unauthorized access or misuse.

**Establish Business Associate Agreements (BAAs).**
For each third-party tracking technology vendor identified that has access to PHI, ensure that a BAA is in place. This agreement should specify the vendor's permitted and required uses and disclosures of PHI, ensuring that the PHI is protected in accordance with HIPAA rules.

- **Benefit:**

BAAs legally bind third-party vendors to uphold the same standards of privacy and security as the primary covered entity, ensuring consistent protection across the digital supply chain.

# Recommendations

**Recommendation 4 - Establish and Maintain BAA management processes for Third-party Providers in Your Digital Supply Chain of websites and webpages:**

**Risk Analysis and Management.**
Address the use of each identified tracking technology in the regulated entity's risk analysis and risk management processes. Implement safeguards, such as sharing ePHI with these vendors and using appropriate access controls.

- **Benefit:**

Regular risk assessments and the implementation of safeguards ensure that vulnerabilities are identified and addressed, enhancing the security of patient data.

**Breach Notification Protocols.**
In the event of an impermissible disclosure of PHI to a third-party tracking technology vendor, have a breach notification protocol in place. This should include notifying affected individuals, the Secretary, and the media (when applicable).

- **Benefit:**

Prompt and transparent breach notifications help mitigate and/or reduce potential damages and maintain trust with patients and stakeholders during and after the incident.

# Recommendations

**Recommendation 5 - Publish Transparent Privacy Notices and Obtaining Patient Consent:**

**Disclosure and Privacy Notices.**
Provide clear, transparent and compliant privacy notices to website visitors when webpages utilize third-party tracking tools, pixels, and technologies on healthcare websites. These notices may need to provide details on the types of data being collected, the purposes of data collection, and the third-party tools involved. Additionally, obtaining explicit consent from patients or website visitors before collecting, processing and/or sharing their data with third-parties may be required. Consult your legal counsel, compliance and other professionals for specific recommendations.

- **Benefit:**

Providing transparent privacy notices and obtaining informed consent ensures that patients and website visitors are aware of and agree to the data collection practices. This not only enhances trust and transparency but also ensures compliance with privacy regulations and other obligations.

# Appendices

## Methodology

Feroot Inspector was used for its ability to gather data directly relevant to answering these questions. Inspector is a crawler, similar to Googlebot, to assess what gets loaded into the browser when a given webpage is requested. It observes and assesses activities of pixels, tracking technologies, tools, libraries, scripts and the like, including: how ubiquitous are they, which specific ones are most prevalent, what PHI/ePHI data they have access to and/or are accessing.

Furthermore, Feroot Inspector also collected information about the publicly accessible software supply chain and its dependencies, including other third-party and downstream fourth-party scripts, additional client-side scripts reading and transferring data, cross-border transfers and much more.

## Data Collection

Feroot Inspector collected data on pixels/trackers over an 4-week period in summer of 2023.

## Analyses

Feroot analyzed the data it collected regarding pixels/trackers collecting and transferring data correlated against: Known banned companies, their applications, pixels/trackers, etc. Handling of privacy and sensitive user data Known business and operational risks related to data breaches and calculated percentages and distributions of the results for the relevant cases of interest.

# Glossary

**Advertising technology (or adtech) -** the term that refers commonly to all technologies, software and services used for delivering and targeting online advertisements.

**Advertising trackers** - a utility, script or program that monitors the performance of advertising campaigns

**Analytic trackers** - a utility, script or program that gathers statistical data from connected web sources for analysis.

(Source: https://linktrack.info/p/ad_tracker)

**Attack Vector** - a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

**Customer Service trackers** - a utility, script or program that gathers and organizes information related to customer activities.

**CCPA** - The California Consumer Privacy Act (CCPA) is a bill that enhances privacy rights and consumer protection for the residents of California, USA.

**Chatbot** - a computer program designed to simulate a conversation with human users, especially over the Internet.

**Code Injection -** the general term for attack types which consist of injecting code that is then interpreted/executed by the application.

**Cross-border data transfers -** The transfer of information, or data, is often referred to as data flows. Placed in a global context, data flows which cross country borders are cross-border data flows.

**Controller** - The data controller is the one who owns the data. They make the decision to collect personal data in the first place.

**Cookies** (Internet) - messages that **web** servers pass to your **web** browser when you visit **Internet** sites. Your browser stores each message in a small file, called **cookie**.txt . When you request another page from the server, your browser sends the **cookie** back to the server.

**Data leaks** - the unauthorized transmission of data from within an organization to an external destination or recipient.

**Data (singular and plural)** - raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.

**Data Protection** - the process of safeguarding important information from corruption, compromise or loss.

**GDPR** - *The General Data Protection Regulation* is a regulation in EU law on data protection and privacy for all individuals and citizens of the European Union (EU) and European Economic Area (EEA).

**Fourth-Party** - someone your third-party vendor outsources to. Some companies call them sub-processors, providers, strategic partners, etc.

**Formjacking** - a term to describe the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout webpages of e-commerce sites.

# Glossary

**HIPAA** - The *Health Insurance Portability and Accountability Act.*

**Information** - data processed, organized, structured or presented in a given context so as to make it useful.

**Informed Consent** - permission for something to happen that is granted with the knowledge of possible consequences, risks and benefits.

**JavaScript** - a programming language commonly used in web development to add dynamic and interactive elements to websites.

**Libraries (Script or JavaScript)** - a file that contains a collection of functions which accomplish some useful task for your webpage.

**Man-in-the-middle attack -** an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

**Malicious code -** an application security threat. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

**Outlier** - a data point that differs significantly from other observations.

**PCI-DSS** - The *Payment Card Industry Data Security Standard (PCI DSS)* is an information security standard for organizations that handle branded credit cards from the major card schemes.

**Personal Data** - any information relating to an identified or identifiable natural person ('data subject'), such as a name, an identification number, location data, an online identifier, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Pixel tracking** - an HTML code snippet which is loaded when a user visits a website or opens an email.

**Privacy -** the state or condition of freedom from being observed or disturbed by other people and having control relating to the use of your own data.

**Processor -** the person, public authority, agency or other body that processes the data on behalf of the data controller.

**Sub-processor** - a processor that makes up a part of a larger processor. Contractual requirements between a processor and sub-processor stay the same as between the data controller and the processor.

**Sensitive Data** - personal data is considered 'sensitive' and is subject to specific processing conditions when the data is revealing racial or ethnic origin; political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

# Glossary

**SaaS -** a method of software delivery and licensing in which software is accessed online via a subscription.

**Trackers -** a utility, script or program that gathers information from social media channels such as blogs, wikis, news sites and micro blogs such as Twitter and social network sites.

**Side-loaded code -** Sideloading is the installation of an application on a mobile device without using the device's official application distribution method. Sideloading can result in an attack with unintended code execution.

**Supply chain attack** - A supply chain attack, also called a value chain or third-party attack, occurs when your system is infiltrated through an outside partner or provider with access to your systems and data.

**Third-Party** - any organization outside of your company that provides a product or service (such as data processing) and has access to your system.

**Trackers or Tags -** objects or scripts used on websites to collect and store data on user behavior for advertising, marketing, site optimization, and security purposes. These scripts are the underlying technology that places tracking cookies on consumers' browsers.

**Web Tracking** - Web tracking is the activity (and ability) of a website to keep track of website visitors using software tools.

**Website -** a location connected to the Internet that maintains one or more pages on the World Wide Web.

**Web Apps or Web-Apps -** a web application is a software application that runs on a remote server.

**Web Form** — a web form or HTML form on a webpage allows a user to enter data that is sent to a server for processing.

**Additional Glossaries**

NICSS Glossary of Common Cybersecurity Terms:
https://niccs.us-cert.gov/about-niccs/glossary

Glossary of Privacy Terms (IAPP)
https://iapp.org/resources/glossary

Common Software and Application Security Terms Explained
https://blogs.grammatech.com/common-software-and-application-security-terms-explained