



# HIPAA compliance alert: Avoid breaches from online trackers on health websites

Wednesday, 20 August

09:00–10:00 PDT

12:00–13:00 EDT

18:00–19:00 CEST



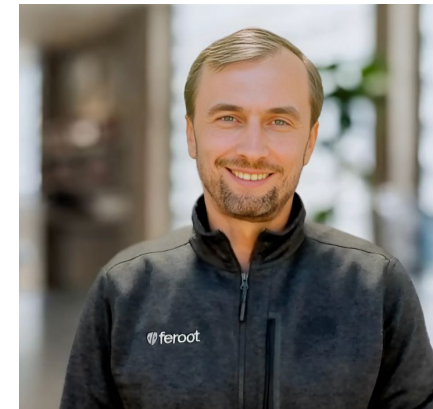
# Meet The Panelists



**Jason Frame**  
Chief Information Officer (CIO)  
Southern Nevada Health District



**Jim Buda**  
Senior Manager  
Insight Insurance



**Ivan Tsarynny**  
CEO / Co-Founder  
Feroot Security



**01**

**Welcome &  
Introductions**

**02**

**Snapshot: PHI &  
Health-Related Incidents  
in 2025 and 2024**

**03**

**What are the Rules?**

**04**

**How Healthcare Websites Leak Data**

a. What actually happens under the hood?

**05**

**Live Review Of Website  
With Real Issues**

**06**

**Lessons from the Trenches: Practical Playbook**

- a. CISO's perspective – Practical Experience
- b. The Assessor's perspective – Before, During and After

What is the Percentage of Websites that use **Online Tracking Technologies (OTT)** such as advertising, analytics and social media tracking pixels?

- 0-20%
- 21-50%
- 51-90%
- 91-100%

# 95%

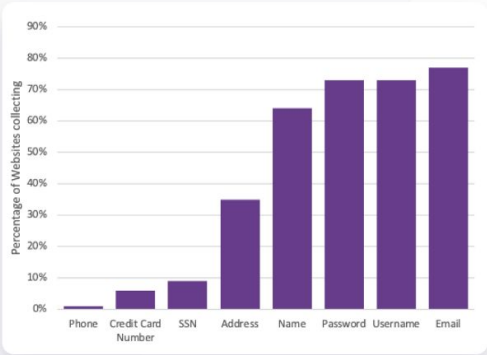
of healthcare websites use Online Tracking Technologies (OTT) such as advertising, analytics, customer service, social media tracking pixels.

[Click Here](#) for the  
full 2024 report



## 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%

All attendees today will be pre-registered to receive the 2025 Annual Healthcare Report upon release.





**Jason Frame**  
CIO  
Southern Nevada  
Health District



- CIO, Southern Nevada Health District – advancing IT strategy, innovation, and public health outcomes.
- Challenge – limited visibility into online tracking technologies and organizational risk exposure.
- Solution – partnered with Feroot in a proof of concept, delivering full visibility and enhanced security posture.



**Jim Buda**  
CISSP, CPA  
IT Risk and Compliance  
Insight Insurance



- Senior Manager, Insight Assurance – delivering strategic audit leadership across highly regulated industries.
- Expertise – 12+ years of experience leading engagements across SOX, SOC, HIPAA/HITRUST, and privacy frameworks.
- Focus – part of Insight Assurance’s 3-step review model, ensuring consistency, quality, and actionable guidance.



Featured on:



Feroot AI found code in DeepSeek's web login page that directly connected it to China Mobile, a company designated as a Chinese military company.



Ivan Tsarynny  
CEO / Co-Founder  
Feroot Security



CNBC News



CSPAN @cspan · 1h

.@ivan\_tsarynny, CEO of Feroot cybersecurity, testifies @USCC\_GOV on the cyber risks of TikTok. He says ByteDance, the parent company of TikTok, uses technology that collects large amounts of U.S. users' data--even from people who have never used TikTok.



TECHNOLOGY

Researchers link DeepSeek's blockbuster chatbot to Chinese telecom banned from doing business in US



The smartphone app DeepSeek page is seen on a smartphone screen in Beijing, Jan. 28, 2025. (AP Photo/Andy Wong, File)

The Associated Press

### Relevant publications:

- [Feroot on New York Times](#)
- [Feroot on Forbes](#)
- [Feroot on Fortune](#)
- [Feroot on ABC Good Morning America](#)
- [Feroot at US Congress](#)
- [Feroot on Wall Street Journal](#)
- [Feroot on Associated Press](#)
- [Feroot on CNBC](#)
- [Feroot on ABC News](#)
- [Feroot on Bloomberg](#)

# Snapshot: PHI & OTT related Incidents in 2025 and 2024

## 2025 Highlights

Organization	Amount	TLDR
Aspen Dental Management	<a href="#">\$18.5m</a>	Tracking tools: Meta Pixel, Google Analytics
BJC HealthCare	<a href="#">Up to \$9.25m</a>	Tracking tools: Meta Pixel, Google Analytics
Eisenhower Medical Center	<a href="#">\$875,000</a>	Meta Pixel shared health data during website searches and interactions.
Group Health Plan (HealthPartners)	<a href="#">\$6m</a>	Pixel violations on websites disclosing PHI.
Loyola University Medical Center	<a href="#">\$2.67m</a>	Pixel tracking on websites shared PHI.
Mount Nittany Health	<a href="#">\$1.8m</a>	Privacy violations via pixels.
University of Rochester Medical Center	<a href="#">\$2.85m</a>	Meta Pixel on website and MyChart portal.
WakeMed Health & Hospitals	<a href="#">\$2.45m</a>	Meta Pixel on MyChart and websites.
Flo Health (vs. Meta)	<a href="#">Damages pending</a>	Meta collected women's health data via app integration.
Blue Shield of California	<a href="#">Class action filed</a>	Certain member data shared with Google's advertising product.

## 2024 Highlights

Organization	Amount	TLDR
DaVita Inc.	<a href="#">\$3.8m</a> (Corrected info and link)	Pixels on patient portals shared dialysis patients' data.
GoodRx	<a href="#">\$25m</a>	OTT disclosure of sensitive health data without consent.
Cerebral (Telehealth)	<a href="#">\$7m</a>	FTC's "first-of-its-kind" ban on using health data for ads
Mount Nittany Health	<a href="#">\$1.8m</a>	Meta Pixel tracked patients' visits without authorization.
Palm Beach Health Network	<a href="#">Lawsuit pending</a>	Meta Pixel collected searches made by patients, appointment details and more
Monument (Alcohol Treatment)	<a href="#">\$2.5m</a>	Addiction treatment data shared with tracking pixels.
Kaiser Permanente	<a href="#">Pending lawsuits</a>	13.4M patients' search terms and other data exposed to Tracking pixels
VillageMD	<a href="#">Lawsuit filed</a>	Online tracking tools collected patient data without proper consent.
Henry Ford Health	<a href="#">\$12.2m</a>	Meta Pixel tracked MyChart portal users from 2020-2023.
University of Rochester Medical Center	<a href="#">\$2.85m</a>	Use of tracking technology on its website and MyChart patient portal.

## Webpages subject to HIPAA rules

**User-authenticated web pages:** Ensure that online tracking technologies are used in compliance with the HIPAA Privacy Rule and are secured in accordance with the HIPAA Security Rule.

**Unauthenticated webpages:** that permit individuals to schedule appointments, use a symptom-checker tool, or log in to patient portal web pages must use online tracking technologies in compliance with the HIPAA Privacy Rule.

## Establish a Business Associate Agreement (BAA)\*

for each online tracking technology (business associates) that create, receive, maintain, or transmit PHI.

**Business Associate Agreement:** outlines the business associate's responsibilities for protecting PHI and complying with HIPAA's Privacy, Security, and Breach Notification Rules.

## Collect individuals' authorization

for any disclosure of PHI to the vendor without BAA in place.

[HHS Guidance](#) – Use of Online Tracking Technologies by HIPAA Covered Entities

Short answer:

# Marketing

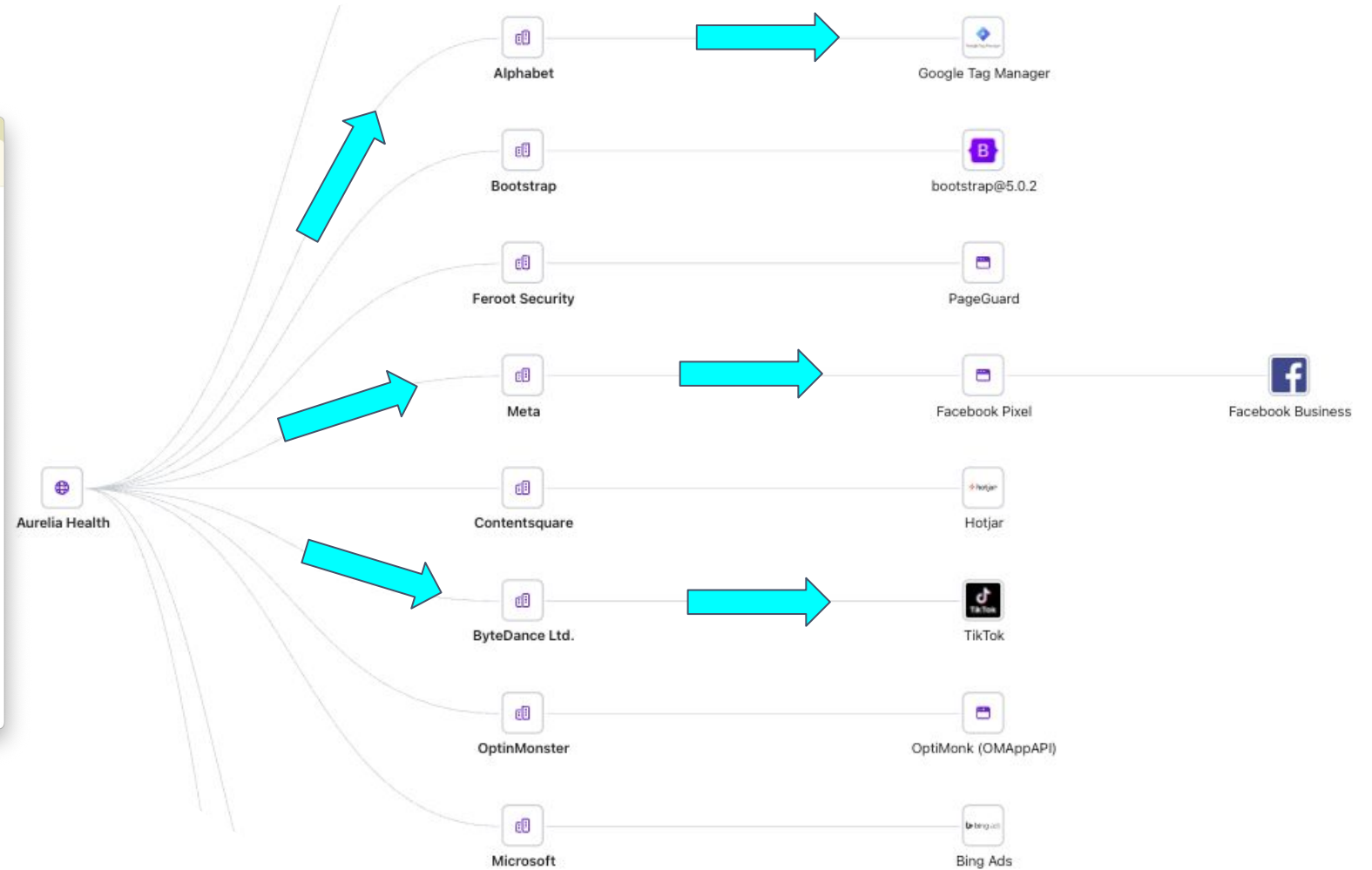
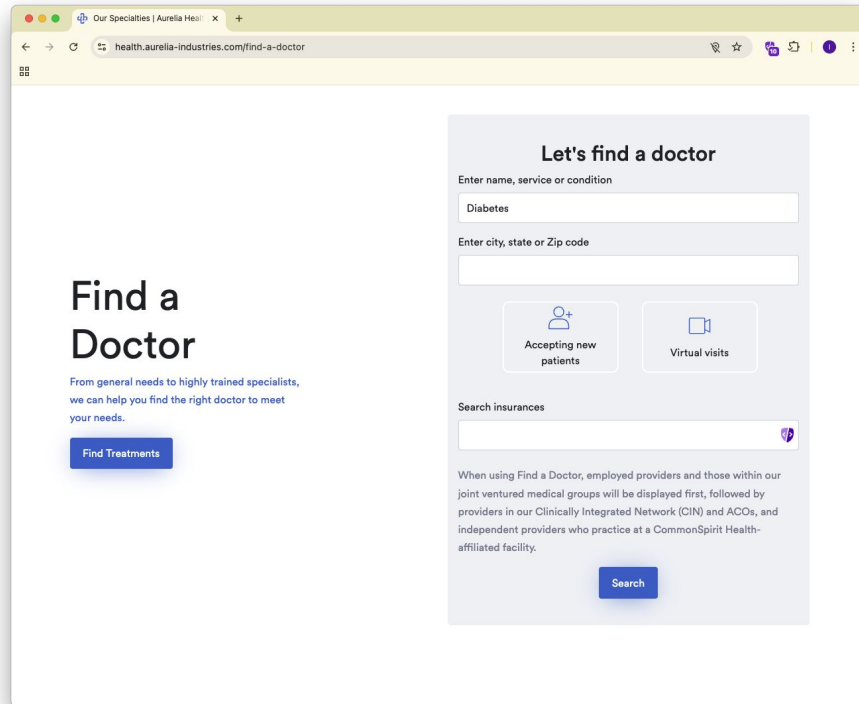
Longer answer:

## MAMA

 Meta Alphabet

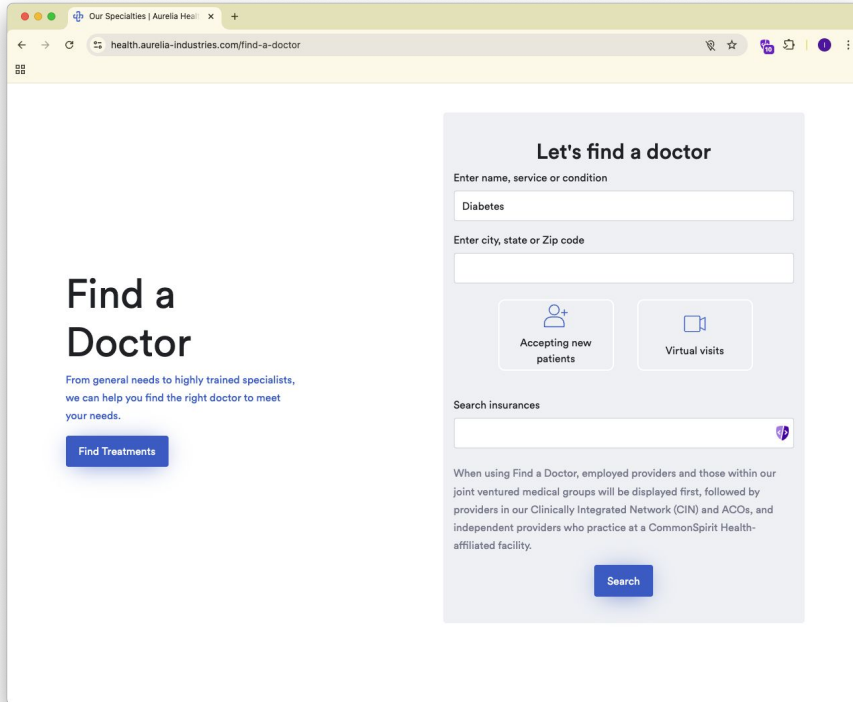
The Long Answer:

**95%** of Healthcare websites use various marketing tracking technologies such as **tracking pixels, analytics scripts and tags** embedded in their websites which often inadvertently collect and transfer PHI, PII and other sensitive information data to third-party vendors.



**Can you show it  
in the real world?**

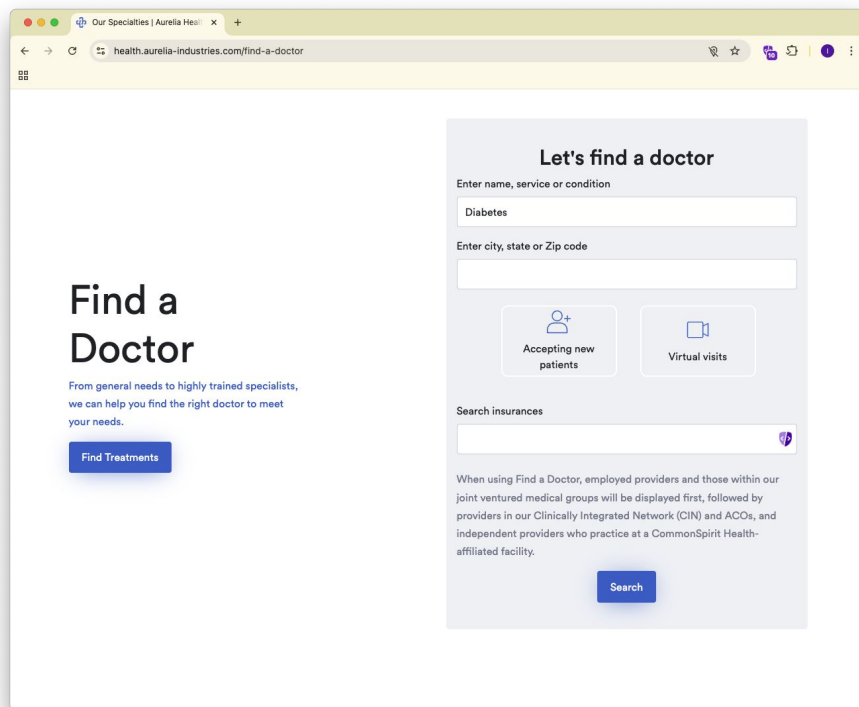




The screenshot shows a web browser window with the URL `health.aurelia-industries.com/find-a-doctor`. The page has a light yellow header and a white main content area. On the left, there is a section titled "Find a Doctor" with a subtext: "From general needs to highly trained specialists, we can help you find the right doctor to meet your needs." Below this is a blue button labeled "Find Treatments".

The main content area features a light gray box titled "Let's find a doctor". Inside this box, there are three input fields: "Enter name, service or condition" (containing "Diabetes"), "Enter city, state or Zip code", and "Search insurances". Below the "Search insurances" field is a small purple icon. There are also two buttons: "Accepting new patients" (with a person icon) and "Virtual visits" (with a video camera icon). At the bottom of the gray box is a blue "Search" button.

Below the "Search" button, there is a paragraph of text: "When using Find a Doctor, employed providers and those within our joint ventured medical groups will be displayed first, followed by providers in our Clinically Integrated Network (CIN) and ACOs, and independent providers who practice at a CommonSpirit Health-affiliated facility."



Our Specialties | Aurelia Health

health.aurelia-industries.com/find-a-doctor

### Find a Doctor

From general needs to highly trained specialists, we can help you find the right doctor to meet your needs.

Find Treatments

#### Let's find a doctor

Enter name, service or condition

Diabetes

Enter city, state or Zip code

Accepting new patients

Virtual visits

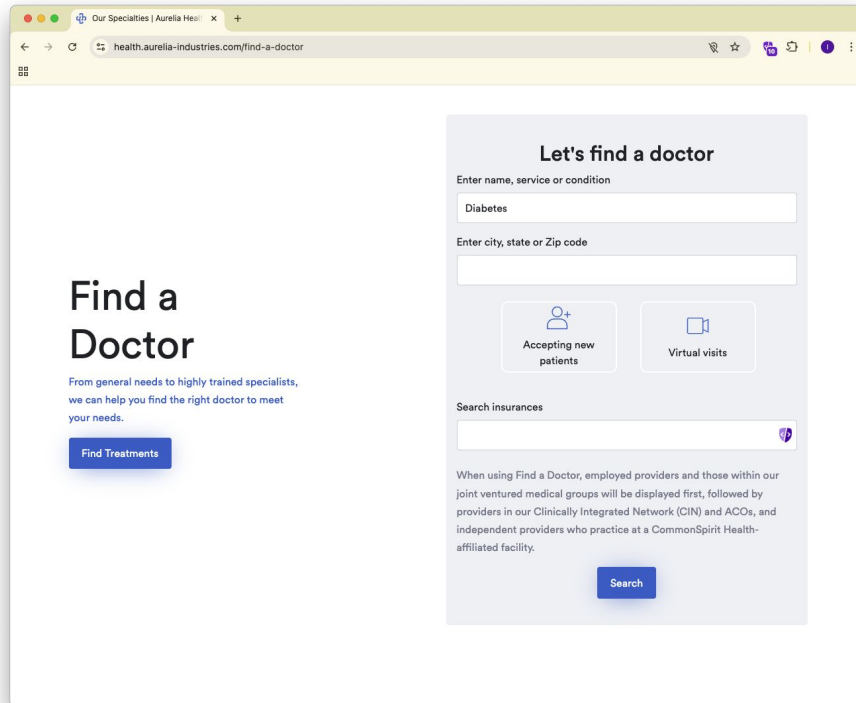
Search insurances

When using Find a Doctor, employed providers and those within our joint ventured medical groups will be displayed first, followed by providers in our Clinically Integrated Network (CIN) and ACOs, and independent providers who practice at a CommonSpirit Health-affiliated facility.

Search

What percentage of websites with user login/registration pages have OTTs actively reading what user are entering?

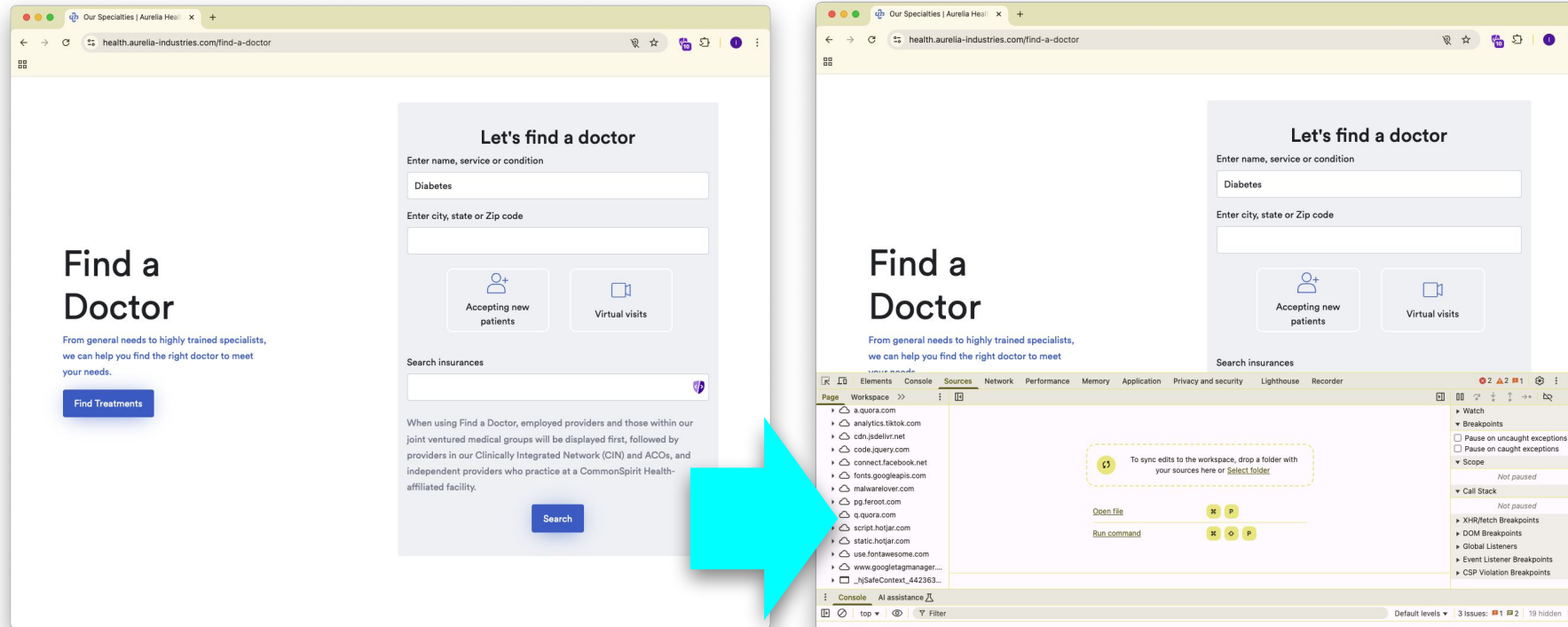
- 31-50%
- 16-30%
- 6-15%
- 0-5%



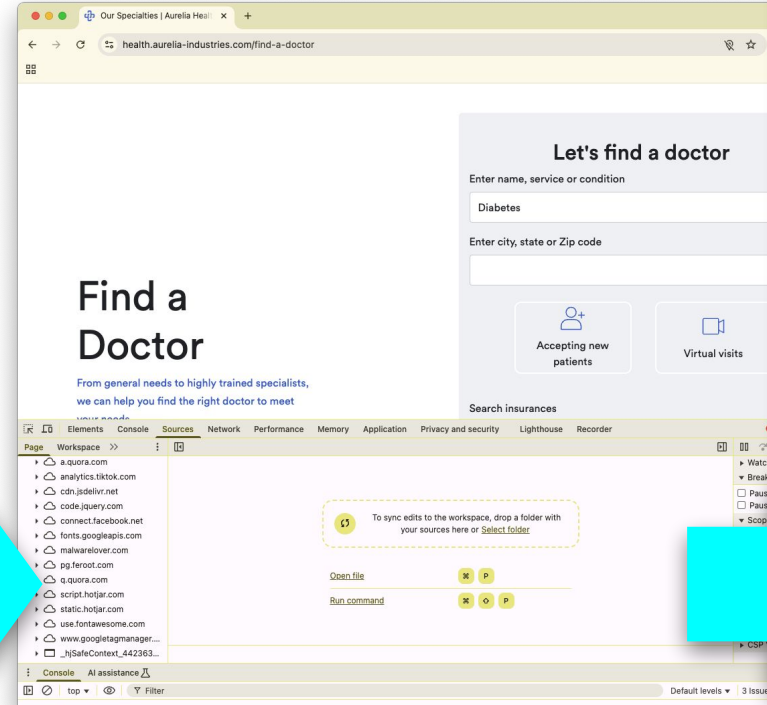
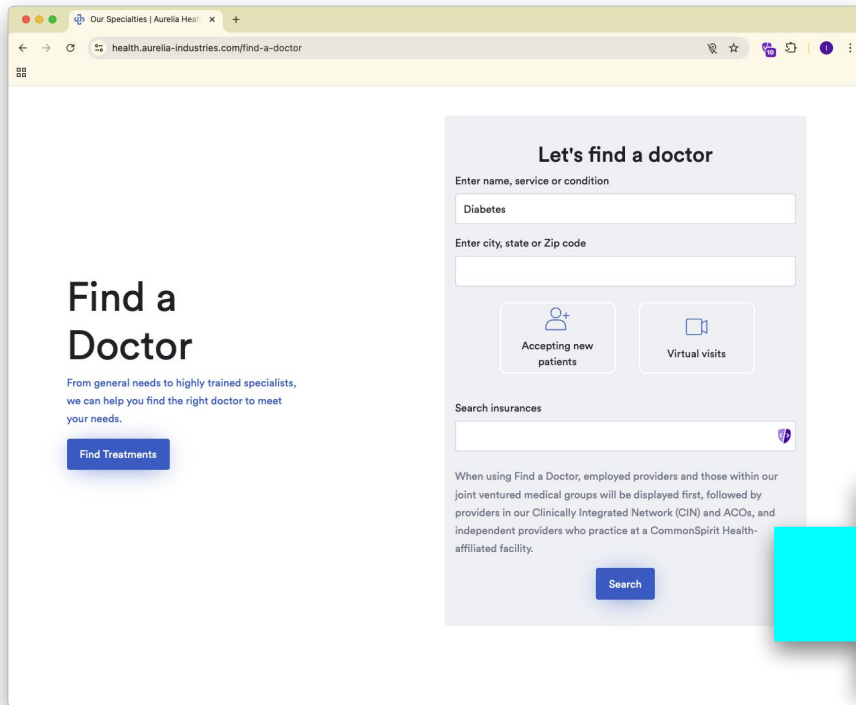
39%

of websites with user login/registration pages have OTTs actively reading what user are entering.

## What Actually Happens Under the Hood?



## What Actually Happens Under the Hood?



Aurelia Health

July 17th, 2025 - August 17th, 2025

VENDORS

12

PRODUCTS

18

THREATS

15

FIRST-PARTY

3

THIRD-PARTY

15

DATA ASSETS

17



























DATA ACCESS

290

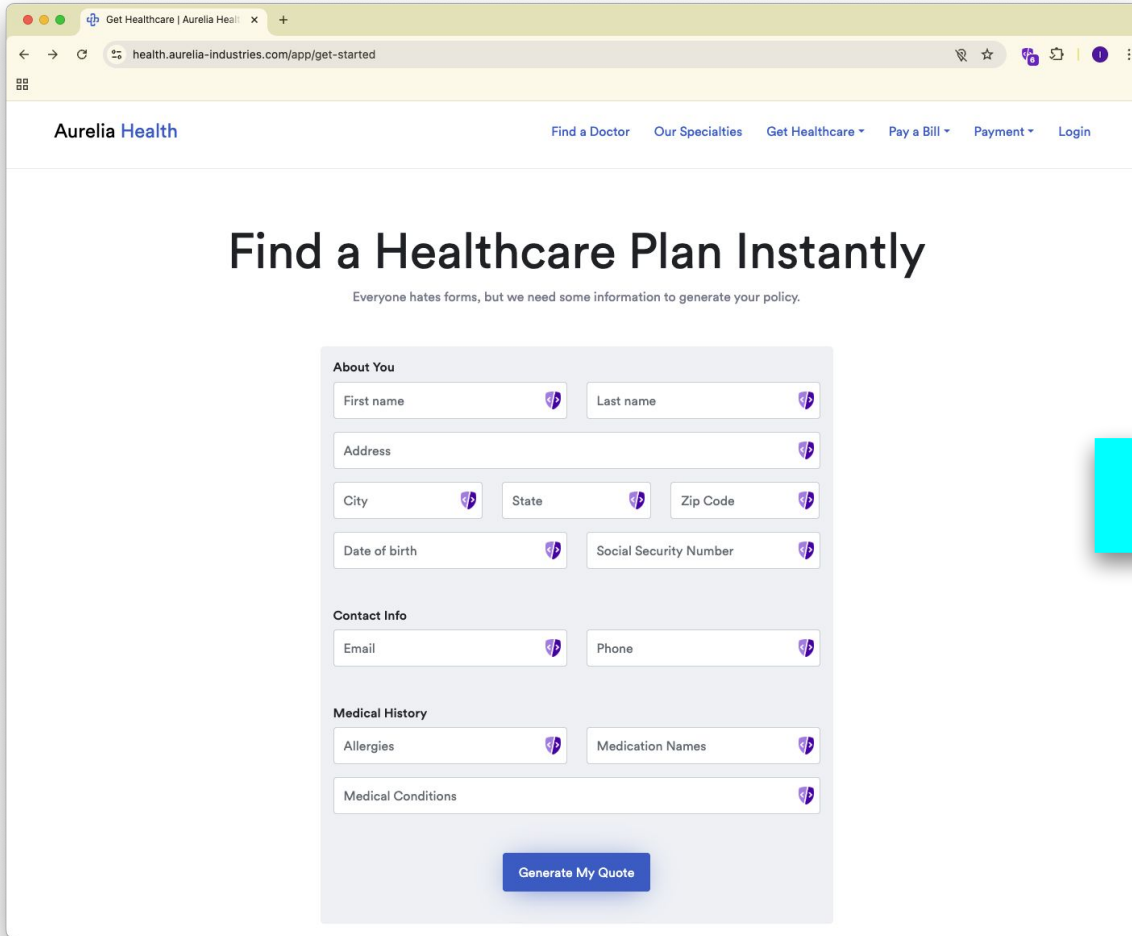
Vendors

Category(Advertising and 4 others)

Details

VENDOR	PRODUCT	CATEGORY	DETAILS
OptinMonster	 OptiMonk (OMAppAPI)	 Analytics	 Third-Party
Microsoft	 Bing Ads	 Advertising	 Third-Party
Meta	 Facebook Business	 Advertising	 Third-Party
	 Facebook Pixel	 Analytics	 Third-Party
Feroot Security	 PageGuard	 Essential	 Third-Party  Data Assets
Contentsquare	 Hotjar	 Analytics	 Third-Party
ByteDance Ltd.	 TikTok	 Social Media	 Third-Party  Data Assets
Alphabet	 Google Tag Manager	 Advertising	 Third-Party

How do Tracking Technologies get “in”?



Get Healthcare | Aurelia Health

health.aurelia-industries.com/app/get-started

Aurelia Health

Find a Doctor Our Specialties Get Healthcare Pay a Bill Payment Login

## Find a Healthcare Plan Instantly

Everyone hates forms, but we need some information to generate your policy.

**About You**

First name Last name

Address

City State Zip Code

Date of birth Social Security Number

**Contact Info**

Email Phone

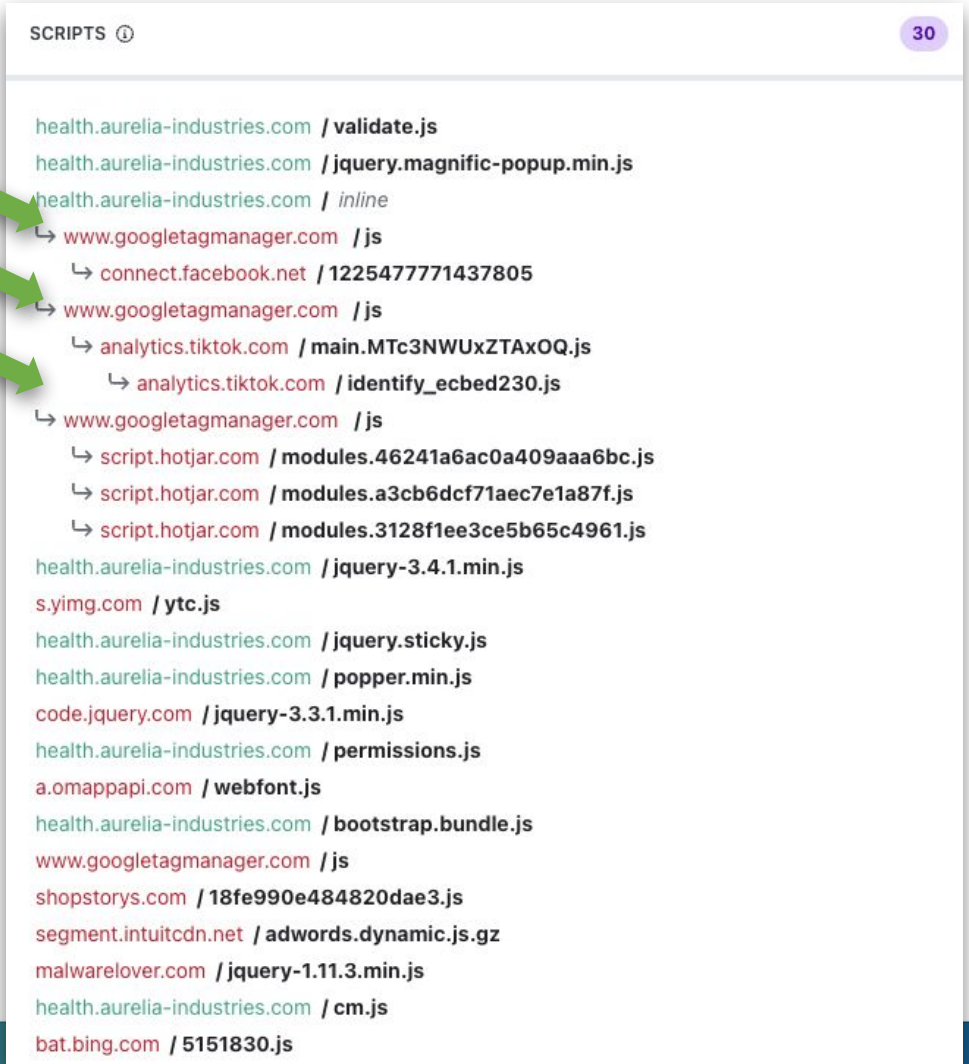
**Medical History**

Allergies Medication Names

Medical Conditions

Generate My Quote

Tag manager  
launches  
tracking  
pixels

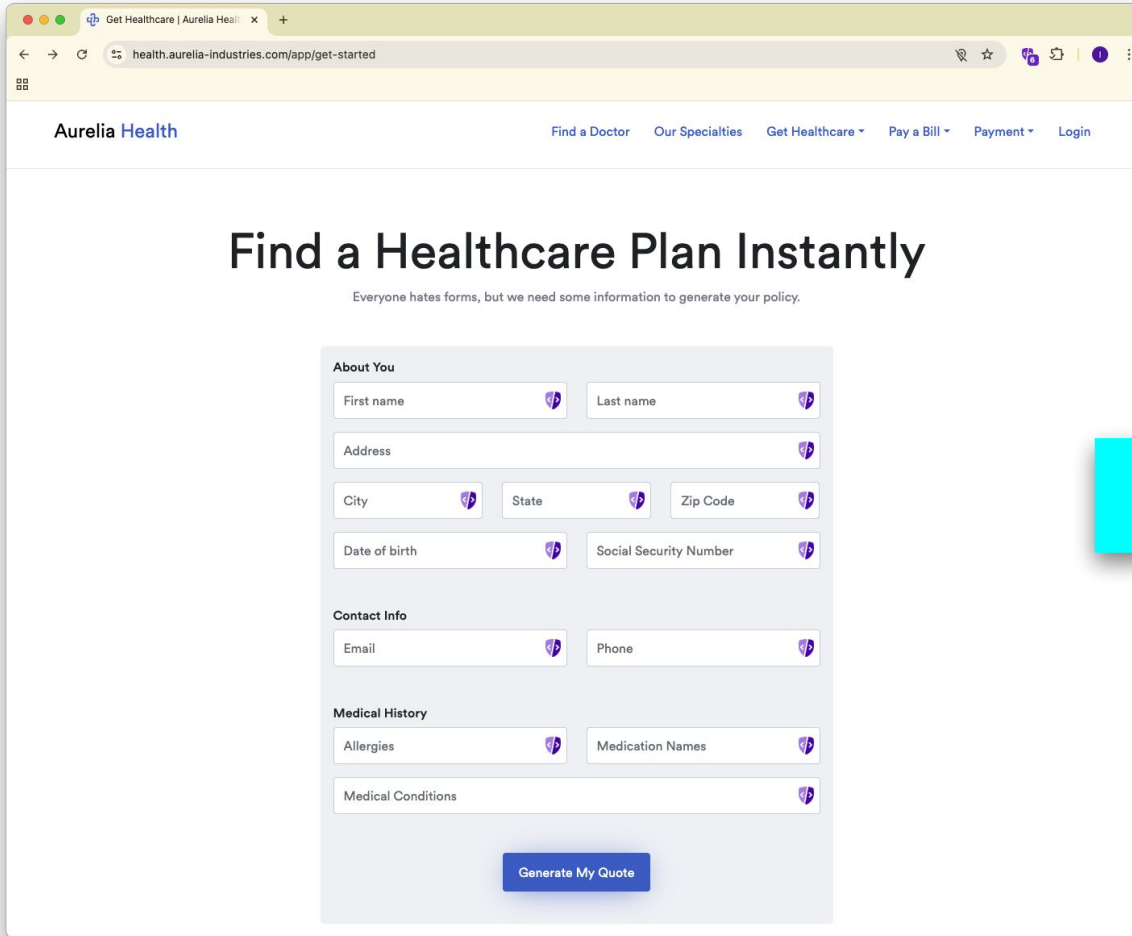


SCRIPTS ⓘ 30

- health.aurelia-industries.com / validate.js
- health.aurelia-industries.com / jquery.magnific-popup.min.js
- health.aurelia-industries.com / inline
  - www.googletagmanager.com / js
    - connect.facebook.net / 1225477771437805
  - www.googletagmanager.com / js
    - analytics.tiktok.com / main.MTc3NWUxZTExOQ.js
    - analytics.tiktok.com / identify\_ecbed230.js
  - www.googletagmanager.com / js
    - script.hotjar.com / modules.46241a6ac0a409aaa6bc.js
    - script.hotjar.com / modules.a3cb6dcf71aec7e1a87f.js
    - script.hotjar.com / modules.3128f1ee3ce5b65c4961.js
- health.aurelia-industries.com / jquery-3.4.1.min.js
- s.yimg.com / ytc.js
- health.aurelia-industries.com / jquery.sticky.js
- health.aurelia-industries.com / popper.min.js
- code.jquery.com / jquery-3.3.1.min.js
- health.aurelia-industries.com / permissions.js
- a.omappapi.com / webfont.js
- health.aurelia-industries.com / bootstrap.bundle.js
- www.googletagmanager.com / js
- shopstorys.com / 18fe990e484820dae3.js
- segment.intuitcdn.net / adwords.dynamic.js.gz
- malwarelover.com / jquery-1.11.3.min.js
- health.aurelia-industries.com / cm.js
- bat.bing.com / 5151830.js



Once Tracking Technologies are “in”, what can they do?



Get Healthcare | Aurelia Health

health.aurelia-industries.com/app/get-started

Aurelia Health

Find a Doctor Our Specialties Get Healthcare Pay a Bill Payment Login

## Find a Healthcare Plan Instantly

Everyone hates forms, but we need some information to generate your policy.

**About You**

First name Last name

Address

City State Zip Code

Date of birth Social Security Number

**Contact Info**

Email Phone

**Medical History**

Allergies Medication Names

Medical Conditions

Generate My Quote

Top frame  
https://health.aurelia-industries.com/app/get-started

Show Invisible Inputs

ACTIVE DATA READ 1

analytics.tiktok.com / main.MTc3NWUxZTAxOQ.js

FIRST-PARTY SCRIPTS DATA ACCESS 9

health.aurelia-industries.com / validate.js  
health.aurelia-industries.com / jquery.magnific-popup.min.js  
health.aurelia-industries.com / jquery-3.4.1.min.js  
health.aurelia-industries.com / get-started inline  
health.aurelia-industries.com / jquery.sticky.js  
health.aurelia-industries.com / popper.min.js  
health.aurelia-industries.com / permissions.js  
health.aurelia-industries.com / bootstrap.bundle.js  
health.aurelia-industries.com / disclaimer.js

THIRD-PARTY SCRIPTS DATA ACCESS 13

connect.facebook.net / fbevents.js  
analytics.tiktok.com / identify\_ecbed230.js  
script.hotjar.com / modules.46241a6ac0a409aaa6bc.js  
connect.facebook.net / 1225477771437805  
analytics.tiktok.com / main.MTc3NWUxZTAxOQ.js  
code.jquery.com / jquery-3.3.1.min.js  
analytics.tiktok.com / events.js  
www.googletagmanager.com / js  
static.hotjar.com / hotjar-2560403.js  
shopstorys.com / 18fe990e484820dae3.js  
malwarelover.com / jquery-1.11.3.min.js  
pg.feroot.com / 07a65452-ee61-4f01-8fe6-356c2cb5110f  
cdn.jsdelivr.net / axios.min.js

City city TEXT

Allergies Allergies TEXT

Medications Medication Names TEXT

State / Province state TEXT

Email Email TEXT

First name First name TEXT

Address Address TEXT

Date of Birth Date of Birth TEXT

ZIP / Postal code zip TEXT

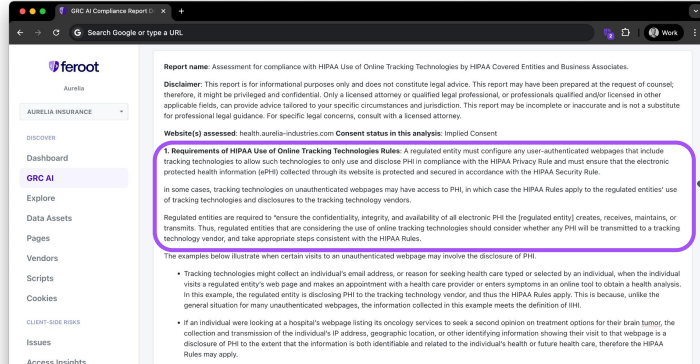
Social Security Number ssn TEL

Last name Last name TEXT

Medical Conditions Medical Conditions TEXT

Phone Phone TEL

## Once Tracking Technologies are “in”, what can they do?



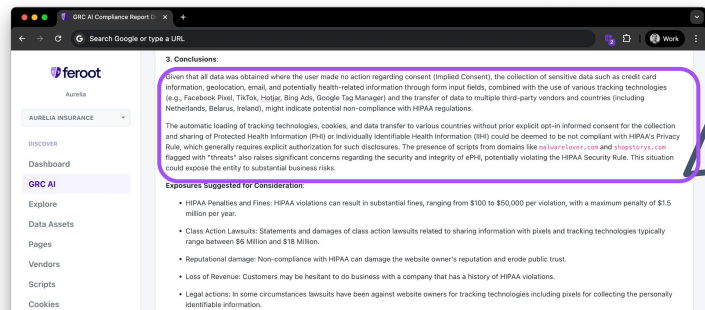
**1. Requirements of HIPAA Use of Online Tracking Technologies Rules:** A regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.

in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors.

Regulated entities are required to “ensure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits. Thus, regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.

Given that all data was obtained where the user made no action regarding consent (Implied Consent), the collection of sensitive data such as credit card information, geolocation, email, and potentially health-related information through form input fields, combined with the use of various tracking technologies (e.g., Facebook Pixel, TikTok, Hotjar, Bing Ads, Google Tag Manager) and the transfer of data to multiple third-party vendors and countries (including Netherlands, Belarus, Ireland), might indicate potential **non-compliance with HIPAA regulations**.

The automatic loading of tracking technologies, cookies, and data transfer to various countries without prior explicit opt-in informed consent for the collection and sharing of Protected Health Information (PHI) or Individually Identifiable Health Information (IIHI) could be deemed to be not compliant with HIPAA's Privacy Rule, which generally requires explicit authorization for such disclosures. The presence of scripts from domains like **malwarelover.com** and **shopstorys.com** flagged with "threats" also raises significant concerns regarding the security and integrity of ePHI, potentially violating the HIPAA Security Rule. This situation could expose the entity to substantial business risks.



**You can't *manage* what  
you don't *measure***

How many OTTs (trackers) are present on average on a healthcare provider's website?

- 0-2
- 3-5
- 6-8
- 9-10

# 10

OTTs (trackers) are present on average on a  
healthcare provider's website

1. **Identify** all webpages subject to HIPAA (and other applicable privacy laws).

2. **Discover** all online tracking technologies OTT's on each webpage subject to HIPAA.

3. **Enter into a Business Associate Agreement (BAA)** for each tracking technology, product, or vendor that creates, receives, maintains, or transmits PHI, or obtain individuals' consent when required.

4. **Prevent:**

- a) Loading of unauthorized vendors, products, and tracking technologies on webpages subject to HIPAA.
- b) Unauthorized access to PHI and other sensitive information.



[Click Here](#) for a Free Assessment of  
OTT Usage on Your Websites



# Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

**Click here: <https://iappwf.questionpro.com/t/AbBPvZ6IRG>**

**Thank you in advance!**

For more information: [www.iapp.org](http://www.iapp.org)

**Attention IAPP Certified Privacy Professionals:**

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: [submit for CPE credits](#).

**Continuing Legal Education Credits:**

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other  
IAPP Web Conferences or recordings  
or to obtain a copy of the slide presentation  
please contact:

**[livewebconteam@iapp.org](mailto:livewebconteam@iapp.org)**