
November 29, 2023

U.S. Securities and Exchange Commission
Office of the Whistleblower (c/o ENF-CPU)
14420 Albemarle Point Place, Suite 102
Chantilly, Virginia 20151
Via Online Portal

Bureau of Consumer Protection
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20508

Consumer Protection Branch
U.S. Department of Justice - Civil Division
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Re: Protected lawful disclosure second addendum on mHealth companies violating privacy laws protecting patients seeking opioid and addiction treatment

To the SEC, FTC, DOJ and HHS:

1. We are lawyers representing Jonathan Stoltman, PhD., a lawful whistleblower who made written disclosures on October 20, 2022 and December 14, 2022 implicating one dozen “mHealth” (mobile health) companies in violations of:
 - a. **HIPAA** (the Health Insurance Portability and Accountability Act of 1996),¹ and

¹ See 42 U.S. Code § 1320d–6, Wrongful disclosure of individually identifiable health information.

Whistleblower Aid is a U.S. tax-exempt, 501(c)(3) organization, EIN 26-4716045.

<https://WhistleblowerAid.org> – Anonymously via **Tor Browser**:

<http://p6ufg73qskew53cglxt6hktyt35rbl46yultzyuytq3tvicywa3plid.onion>

Contact via **SecureDrop** over Tor: <http://whistlebloweraid.securedrop.tor.onion> – via **Signal App**: +1 201-773-1371

-
- b. **“Part 2,”** the federal statute and regulations requiring the confidentiality of **Substance Use Disorder (“SUD”)** patient records, including Opioid Use Disorder.²
2. **Disclosure Addendum:** Our client has produced an update to his original report, titled **Privacy Report 2.1: Websites for Opioid Addiction Treatment and Recovery Services: Data Sharing and Privacy Risks**. Our client obtained this information using entirely lawful and open-source methods. Our client’s evidence is not based on trade secrets, nor on any internal or proprietary corporate information. None of the evidence or materials presented here are privileged in any way.³
3. This new report builds on the prior report by adding a new time point where tracker use is measured and adding additional companies employing these tracking technologies, specifically which have received funding from the National Institute of Health.⁴
4. The use of online session tracking tools by medical care providers and other industries has continued to make news since our last disclosure on this issue:
- a. The FTC fined GoodRx⁵ and BetterHelp⁶ for sharing customer health data.
 - b. Online mental health providers Cerebral⁷ and Monument⁸ have reported violating customer privacy rights.

² See 42 U.S. Code § 290dd–2 - Confidentiality of records; see also 42 C.F.R. Part 2, Confidentiality of Substance Use Disorder patient records.

³ Our client is not a lawyer. None of the materials presented here were obtained from lawyers, or in communications in which lawyers were present. None of the materials are marked “Attorney-Client Privileged” or similar. None of the materials concern legal matters. Therefore there is no reason to suspect that any of the materials presented are in any way privileged.

⁴ <https://seed.nih.gov/>

⁵

<https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>

⁶

<https://www.ftc.gov/business-guidance/blog/2023/03/ftc-says-online-counseling-service-betterhelp-pushed-people-handing-over-health-information-broke>

⁷ Tim Starks, *Online mental health provider's use of tracking tech highlights dangers*, The Washington Post, Mar. 13, 2023,

<https://www.washingtonpost.com/politics/2023/03/13/online-mental-health-provider-use-tracking-tech-highlights-dangers/>

⁸ Zach Whittaker, *Alcohol recovery startups Monument and Tempest shared patients' private data with advertisers*, Techcrunch, Apr. 4, 2023,

<https://techcrunch.com/2023/04/04/monument-tempest-alcohol-data-breach/>

-
5. Dr. Stoltman's concerns about privacy violations in the addiction treatment context remain timely. Populations seeking treatment for addiction are among the most vulnerable to backlash or retaliation if their privacy is violated and information about their substance use is disclosed.
 6. **Enclosures:** Attached is a .pdf file of Privacy Report 2.1
 7. Please help to ensure our client never faces retaliation for making these lawful disclosures. Our client is entitled to legal protections against retaliation under statutes, regulations, and common law authorities including, but not limited to, the Sarbanes-Oxley Act,⁹ the Dodd-Frank Act.¹⁰
 8. Please feel free to contact us using the contact information below.

Sincerely,



Andrew P. Bakaj
Senior Counsel

[REDACTED]
[REDACTED]



Kyle Gardiner
Senior Counsel

[REDACTED]
[REDACTED]

Enclosures: As stated

END OF DISCLOSURE

⁹ 18 U.S.C. § 1514A. See also 29 C.F.R. 1980.102.

¹⁰ 15 U.S.C. § 78u-6(h)(1). See also 17 C.F.R. 240.21F-2.

Privacy Report 2.1

WEBSITES FOR OPIOID ADDICTION TREATMENT AND RECOVERY SERVICES: *DATA SHARING AND PRIVACY RISKS*

Jonathan JK Stoltman, PhD

Date: February 15, 2024

OPIOID
POLICY
INSTITUTE

opioidpolicy.org

Opioid Policy Institute

The Opioid Policy Institute is a research think tank that uses a multi-pronged approach to better understand the gaps in treatment and recovery services. Our current areas of focus include technology and stigma/discrimination.

To learn more about our work, visit us at opioidpolicy.org.

Disclosures

This document is informational, educational, and does not constitute legal advice.

Contents

Executive Summary.....	4
Relevant news since Report 2 was released in November 2022	5
The Current Report.....	6
Key Findings	7
Specific Aims.....	8
Methodology	9
Primary Privacy Analysis: Blacklight	11
Secondary Analysis	12
Related Meta (Facebook) Data	12
Statements About Privacy.....	12
Figure 1. Summary Table.....	13
Results.....	13
Summary.....	13
Ad Trackers.....	15
Figure 2. Ad Trackers.....	15
Third-Party Cookies.....	16
Figure 3. Third-party Cookies	16
Meta (Facebook) Pixel.....	17
Google Analytics.....	17
Keylogging	17
Session Recording	17
Ad Tech Companies	17
Statements About Privacy.....	18
Company responses	19
Conclusion.....	20
Appendix	21
SBIR & STTR Benefits.....	21
Understanding SBIR/STTR Funding	21
Understanding SBIR/STTR Grant Funding	22
Understanding SBIR/STTR Grant Review and Decisions.....	22
New Regulations	22
Information Related to NIDA SBIR/STTR Grants.....	23

Executive Summary

While drug overdose deaths continue to surge across the country, access to evidence-based care remains limited for people who use drugs. Members of this historically marginalized, vulnerable population still face stigma and discrimination from healthcare professionals, policymakers, and laypeople in addition to legal jeopardy, as substance use remains criminalized throughout most of the United States. To address the longstanding opioid crisis we are facing, access to addiction treatment and recovery support must be increased, despite -- and because of -- these external factors.

For these reasons, it is *deeply problematic* that digital health services, a potentially important element in increasing access to lifesaving care, have been violating the privacy of patients seeking care.

Addiction health privacy is widely considered to be a core component of treatment and recovery – and has been since long before digital health services were an option. Addiction health privacy rests on these tenets:

- Patients and providers expect the right to access treatment without worrying that their records will be used to take away their children, housing, employment, insurance, public benefits, or freedom.
- Patients and providers expect that statements about privacy, security, and confidentiality are true.
- Patients and providers expect that health information will be protected, not provided to advertising and social media companies so that they may be tracked and further discriminated against.
- Patients and providers expect that the allocation of federal money to these services includes a thorough evaluation of the platform to minimize harm for anyone using or learning about these services.

As discussed in [Report 2](#), violating patient privacy can cause irreparable damage to the patient and the industry as trust is broken in online

approaches to treatment and recovery supports, further isolating vulnerable patients and creating more barriers to help.

We must do better.

Since our landmark report (**Report 2**) was released in Nov 2022, much has happened in the privacy and telehealth space. However, more work is needed to protect people using these services. This addendum, **Report 2.1**, adds additional timepoints to Report 2 while also extending our database to include all digital health products with SBIR/STTR funding from NIDA (National Institute on Drug Abuse, a branch of NIH) that include patient facing services or that a patient would reasonably access.

Relevant news since Report 2 was released in November 2022

- On December 1, 2022, the HHS Office of Civil Rights released guidance related to online tracking of people seeking medical care.^{1, 2} This put a spotlight on tracking across websites and mobile apps, which are covered entities under HIPAA.
 - The key takeaway: ***“Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules...the Privacy Rule does not permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures.”***³
 - Website tracking technologies, as discussed in the bulletin, include the following: *cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts.*

¹ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

² <https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html>

³ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

- The FTC has taken action against select digital mental health companies. Relevant actions include:
 - **GoodRx**⁴
 - **BetterHelp**⁵
- The FTC has acted under the Opioid Addiction Recovery Fraud Prevention Act⁶ related to unsubstantiated health claims and deceiving consumers. The affected companies are these:
 - **R360**⁷
 - **AWAREmed Health & Wellness Resource Center**⁸
- Select services have self-disclosed HIPAA privacy violations related to the use of website tracking technologies included in our reports:
 - **Cerebral**^{9, 10}
 - **Monument (Tempest)**¹¹

The Current Report

Using the publicly available [Blacklight](#) tool developed at The Markup,¹² we analyzed the websites of 22 virtual care platforms for opioid use disorder (OUD) that provide treatment or recovery services (hereinafter referred to as “OUD mHealth websites”).

- 12 websites were in the original Report 2 and now have data from six timepoints over 24 months.
- 10 websites have only the most recent datapoint (March 2023).

⁴ <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>

⁵ <https://www.ftc.gov/business-guidance/blog/2023/03/ftc-says-online-counseling-service-betterhelp-pushed-people-handing-over-health-information-broke>

⁶ <https://www.ftc.gov/legal-library/browse/statutes/opioid-addiction-recovery-fraud-prevention-act-2018>

⁷ https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-hits-r360-its-owner-38-million-civil-penalty-judgment-preying-people-seeking-treatment-addiction?utm_source=govdelivery

⁸ <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-sues-medical-clinic-its-owner-false-or-unsubstantiated-claims-its-treatment-could-cure-addiction>

⁹ https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf

¹⁰ <https://www.washingtonpost.com/politics/2023/03/13/online-mental-health-provider-use-tracking-tech-highlights-dangers/>

¹¹ <https://www.documentcloud.org/documents/23741051-monument-breach-notification>

¹² “The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society.” About Us, The Markup, <https://themarkup.org/about> (last visited Aug. 17, 2022).

Key Findings

- In January 2024, the 22 websites averaged 76,419 total visits.
- These companies have received a combined \$1.03 billion in public and venture capital funding.
 - 13 companies received NIH/NIDA SBIR/STTR funding totaling \$16,701,340.
- The potential data collection and sharing varied greatly *between* and *within* services over the 24-month observation period, potentially complicating patients' and providers' ability to evaluate these services' privacy standards.
 - 20/22 OUD mHealth websites hosted tracking technology that share identifying information with third parties.
 - 55.5% of companies used a Meta (Facebook) Pixel at some time during the 24-month observation period.
 - Meta's policy prohibits services that handle sensitive, health-related information from using Meta (Facebook) Pixel.
 - 72.7% used Google Analytics at some point during the 24-month observation period.
 - Google's policy is that Google Analytics should not be used to collect data with personally identifiable information or protected health information.
- Many of the OUD mHealth websites marketed themselves as "private," "secure," "100% confidential," or "discreet," or include a HIPAA "badge" on their website, in their Meta (Facebook) advertisements, or through Google Ads.

The full data set is available here: <https://airtable.com/shrTTGHK3iDpgw2oo>

Specific Aims

This report aims to describe actual data collection practices used by websites for addiction treatment and recovery services. By highlighting this, we hope policymakers will better understand the need for additional oversight and enforcement of privacy protections in this area.

This report meaningfully builds upon our previous work in two important ways:

1. The inclusion of all NIDA SBIR/STTR funded digital health products that include patient-facing services or that a patient would reasonably access when their clinic uses these services.
 - **For more information about the SBIR/STTR program, see the Appendix.**
2. The inclusion of an additional time point for services included in Report 2 that occurs after guidance from the OCR and FTC action regarding health data privacy practices.

Methodology

We identified 22 websites that offer a virtual platform for addiction treatment or recovery services.

Services	URL	
Original Report 2	Bicycle Health	bicyclehealth.com
	Boulder*	boulder.care
	Bright Heart Health	brighthousehealth.com
	Confidant Health	confidanthealth.com
	DynamiCare Health*	dynamicarehealth.com
	Kaden#	kadenhealth.com
	Loosid	loosidapp.com
	Ophelia	ophelia.com
	PursueCare	pursuecare.com
	reSET-O*#	resetforrecovery.com/patient
	SoberGrid*#	sobergrid.com
Workit Health*	workithealth.com	
New to Report 2.1	Chess Health*	chess.health
	Eleanor Health	eleanorhealth.com
	Enhearten*	enhearten.com
	Marigold Health*	marigoldhealth.com
	OARS+CM*	q2i.com/oars-cm
	RAE Health*	raehealth.com
	Recovery Pad*	recoverypad.com
	Sonara*	sonarahealth.com
	Talkiatry	talkiatry.com
	We the Village*	wethevillage.co

* NIDA SBIR/STTR Funded

No longer operating in the same capacity (Feb 2024)

About the websites and their companies. These 22 OUD mHealth websites and their companies cover a range of approaches to addiction treatment and recovery services. Most websites have a corresponding mobile app that provides additional services. Many services offer access to medical providers who prescribe medication for opioid use disorder (MOUD). Services also offer behavioral therapy and coaching.

By many metrics, these websites are substantial services:

1. On average, the services with reported external funding have raised \$73.6 million in funding.
 - a. Approximate total funding: \$1.03 billion
 - b. Range: \$5.3 million – \$409 million
2. Since 2017, 13 services received public funding from the National Institutes of Health (NIH) through the National Institute on Drug Abuse (NIDA) SBIR/STTR funding mechanism.
3. In January 2023, the websites averaged 76,419 visits.
 - a. Approximate total visits: 1,604,800
 - b. Range: 1,200 – 759,000

For information, including which states they operate in and what specific services are offered, please visit: <https://airtable.com/shrTTGHK3iDpgw2oo>

Selection criteria. We selected these 22 websites for study because (a) their companies have received significant venture capital or funding from the National Institutes of Health (NIH), (b) they enabled comparison with services that received this funding, (c) they have been covered in other research about privacy and online access to addiction treatment or recovery services.

Primary Privacy Analysis: Blacklight

In order to conduct the primary privacy analysis, we used a free tool called Blacklight, developed in 2020 by researchers and journalists at The Markup to provide the public with a real-time privacy inspector for websites.¹³ Blacklight performs an automated inspection of a website to reveal the specific user-tracking technologies on the site and the recipients of the data; it does not provide a definitive investigation of all privacy issues.¹⁴ We focused our analysis on ad trackers, third-party cookies, session recording, Meta (Facebook) Pixel, and Google Analytics. *Blacklight analysis does not show whether the OUD mHealth websites affirmatively installed all the tracking technologies.*

Blacklight data was collected at six time points:

1. March 2021
2. November 2021
3. June 2022
4. July 2022
5. September 2022
6. March 2023*

*New to this report

¹³ *Blacklight: A Real-Time Website Privacy Inspector* by Surya Mattu, THE MARKUP, <https://themarkup.org/blacklight> (last accessed Aug. 17, 2022).

¹⁴ Surya Mattu and Aaron Sankin, *How We Built a Real-time Privacy Inspector*, THE MARKUP (Sept. 22, 2020), <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector>.

Secondary Analysis

Related Meta (Facebook) Data

To further understand whether Meta (Facebook) *actually* received data from these websites, we used an approach similar to the investigation led by Grace Oldham and Dhruv Mehrotra at Reveal:¹⁵

- On August 25, 2022, Jonathan JK Stoltman created a Facebook profile (“Bill Wilson”) and Chrome profile (with no plugins, a clean browser, and a clean cache) to use exclusively for data collection related to analysis for this research.
- On April 12, 2023, they logged in to the new Facebook profile and left the tab open, then visited the 22 OUD mHealth websites in this report. They simulated the behavior of a potential patient or provider by clicking through various portions of the website. They filled out provider and patient forms when available.
- On April 14, 2023, they used Meta’s Privacy Center to download and review the “Off-Facebook Activity” to analyze what data Meta (Facebook) indicated was associated with these companies.
- On April 14, 2023 each site was revisited with the [Meta Pixel Helper Chrome plug-in](#) installed. The Meta Pixel Helper is a troubleshooting tool that helps validate the Meta pixel implementation.

Statements About Privacy

We analyzed various datasets to better understand how services represent themselves as private, confidential, secure, discreet, or “HIPAA compliant” including:

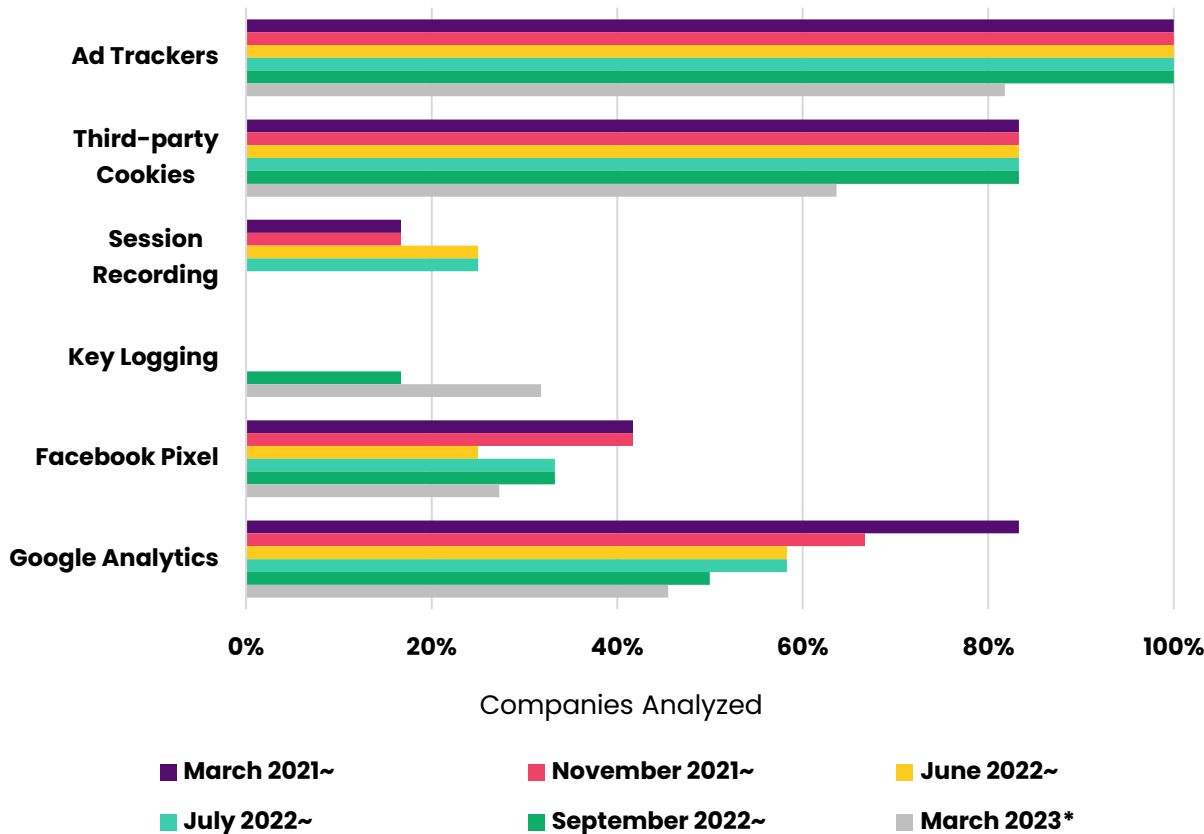
- Meta (Facebook) Ad Library
- Google Ads Transparency Center
- The websites themselves*

*Privacy policies excluded from analysis of the website

¹⁵ Grace Oldham and Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL, (June 15, 2022) <https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/>.

Results

Figure 1. Summary Table



Summary

- **81.8%** of websites used **ad trackers** during March 2023.
- **83.4%** used **ad trackers** at some point during the 24-month observation period.
- **63.6%** of websites used **third-party cookies** during March 2023.
- **77.3%** used **third-party cookies** at some point during the 24-month observation period.
- **31.8%** of websites used **keylogging** during March 2023.

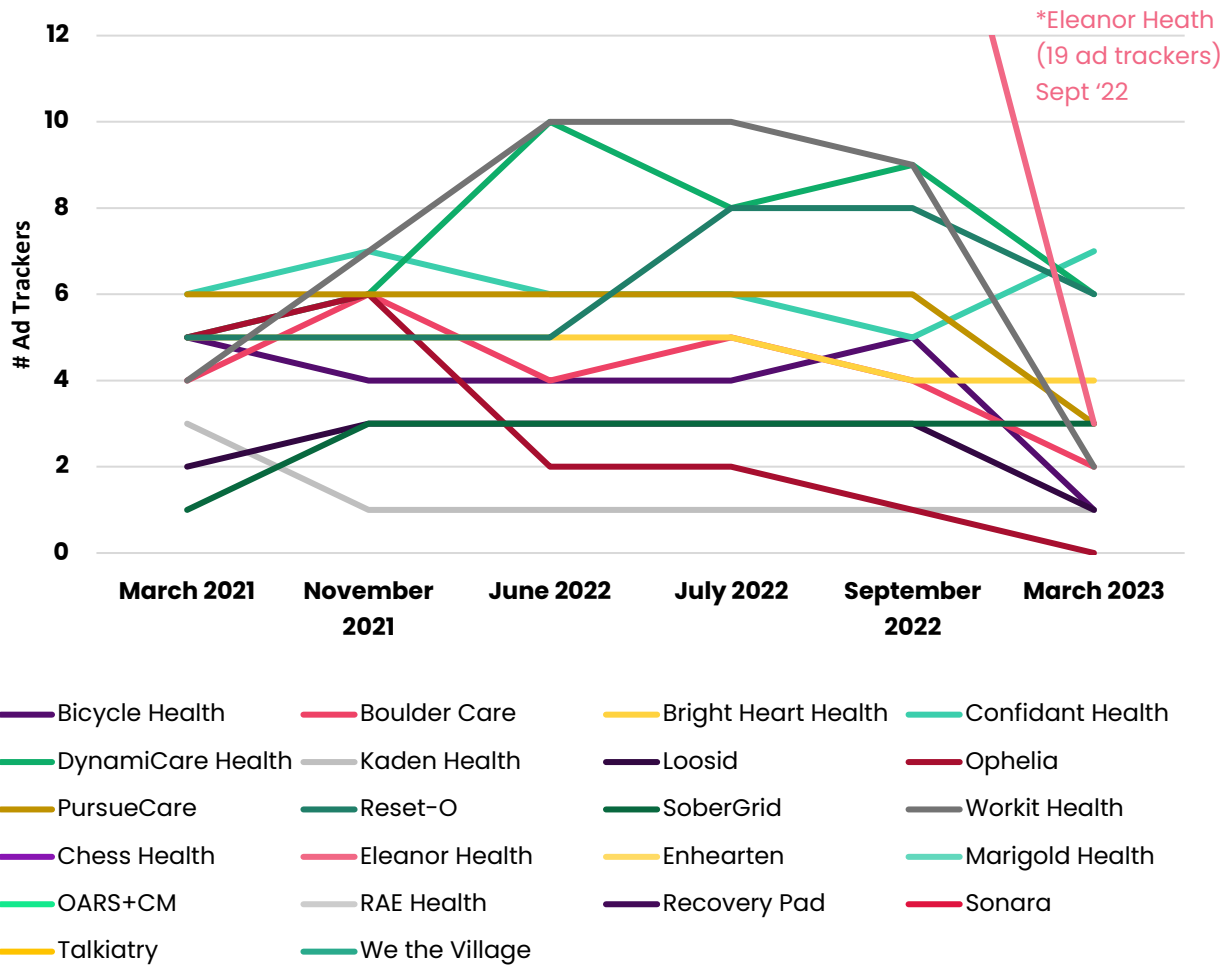
- **31.8%** used **keylogging** at some point during the 24-month observation period.
- **0%** of websites used **session recording** during March 2023.
- **18.2%** used **session recording** at some point during the 24-month observation period.
- **27.3%** of websites used **Meta (Facebook) Pixel** during March 2023.
 - **31.8%** websites appeared in **“Off Facebook” Activity** log in April 2023.
- **54.6%** used **Meta (Facebook) Pixel** at some point during the 24-month observation period.
- **45.5%** of websites used **Google Analytics** during March 2023.
- **72.7%** used **Google Analytics** at some point during the 24-month observation period.
- **61.2%** of websites mentioned privacy or related concepts when describing their service.
- **40.9%** of websites had a HIPAA badge or statement about HIPAA “protecting” data.
- **22.7%** had Meta (Facebook) and/or Google advertisements that mentioned privacy or related concepts.

The full data set is available here: <https://airtable.com/shrTTGHK3iDpgw2oo>

Ad Trackers

- **81.8%** of websites used **ad trackers** during March 2023.
- **83.4%** used **ad trackers** at some point during the 24-month observation period.
- The number of ad trackers used by each service was highly variable across time between and within services (range: 0-19).

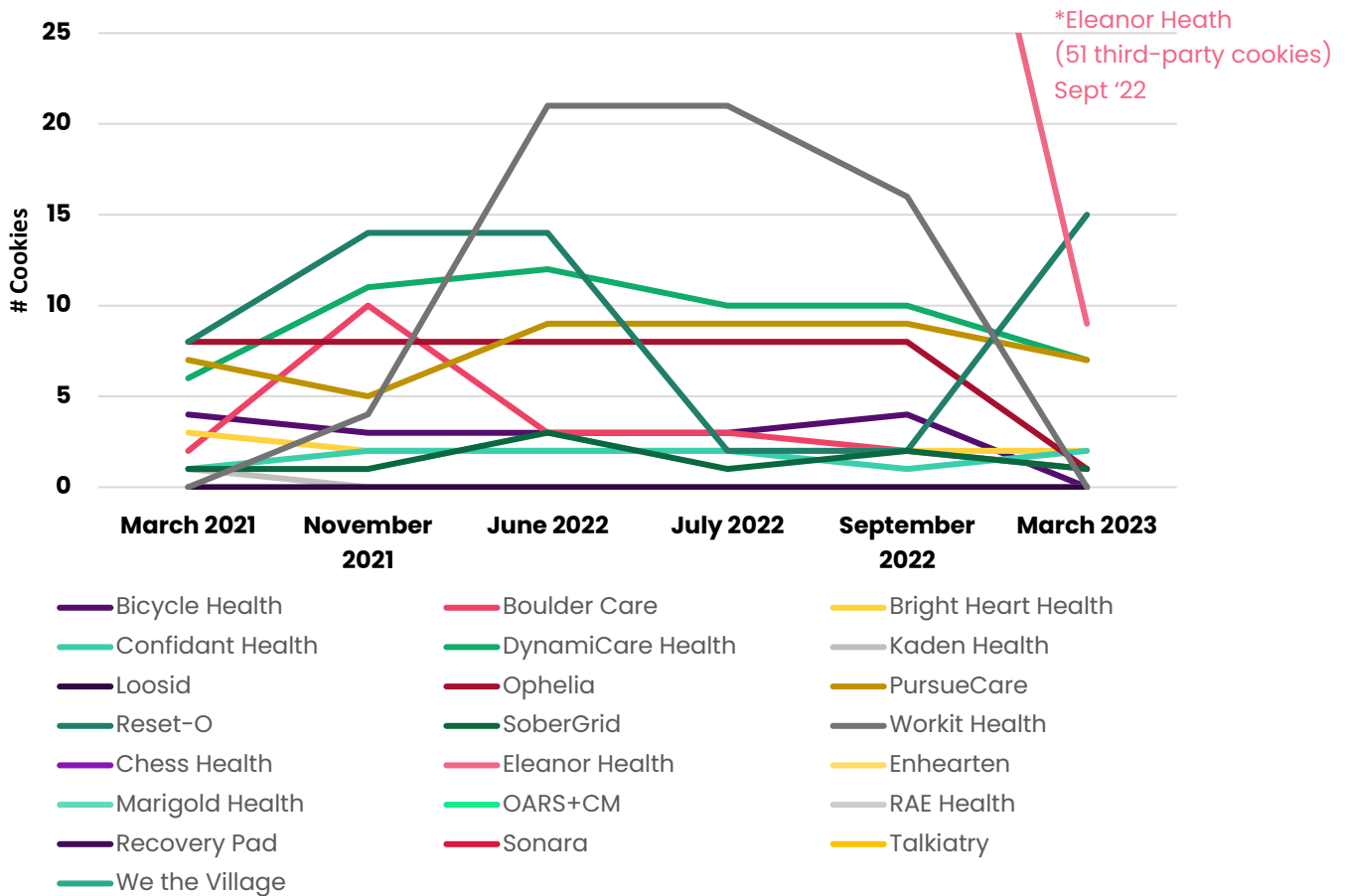
Figure 2. Ad Trackers



Third-Party Cookies

- **63.6%** of websites used **third-party cookies** during March 2023.
- **77.3%** used **third-party cookies** at some point during the 24-month observation period.
- The number of third-party cookies used by each service was highly variable across time between and within services (range: 0-51).

Figure 3. Third-party Cookies



Meta (Facebook) Pixel

- **27.3%** of websites used **Meta (Facebook) Pixel** during March 2023.
 - **31.8%** of websites appeared in “**Off Facebook**” **Activity** log in April 2023.
- **54.6%** used **Meta (Facebook) Pixel** at some point during the 24-month observation period.
- Use of the Meta (Facebook) Pixel was highly variable across time between and within services.

Google Analytics

- **45.5%** of websites used **Google Analytics** during March 2023.
- **72.7%** used **Google Analytics** at some point during the 24-month observation period.
- Use of **Google Analytics** was highly variable across time between and within services.

Keylogging

- **31.8%** of websites used **keylogging** during March 2023.
- **31.8%** used **keylogging** at some point during the 24-month observation period.
- Use of **keylogging** *increased* across time.

Session Recording

- **0%** of websites used **session recording** during March 2023.
- **18.2%** used **session recording** at some point during the 24-month observation period.
- Use of **session recording** *decreased across time*.

Ad Tech Companies

- **21/22** websites sent data to ad tech companies during March 2023 observation.

Statements About Privacy

- **15/22** websites mentioned privacy or related concepts when describing their service.
- **9/22** websites had a HIPAA badge or statement about HIPAA “protecting” data.
- **4/22** had Meta (Facebook) advertisements that mentioned privacy or related concepts.
- **4/22** had Google advertisements that mentioned privacy or related concepts.

Company responses

We reached out to the companies for their responses to issues with data sharing and privacy. Responses are available <https://airtable.com/shrTTGHK3iDpgw2oo>

Conclusion

Our analysis shows that most of the 22 major OUD mHealth websites, which host thousands of visitors per month, are sharing individually identifying information with third-party advertisers. Information that identifies someone as seeking or receiving treatment for addiction or recovery support is *highly sensitive* and traditionally subject to strict privacy protections. These privacy protections exist because this information can be used against the individual's best interest, including in criminal investigation or prosecution, deportation proceedings, family surveillance and child welfare investigations, or discrimination in housing, employment, or benefits. These same privacy considerations apply to information collected by OUD mHealth websites, but despite marketing themselves as "private" and "confidential," they are not meeting the same privacy standards.

Ensuring websites comply with existing privacy standards is essential because these websites provide ways to seek addiction treatment. Internet searches are an increasingly common ways to seek medical advice, including help with reducing drug use. Searching for opioid addiction treatment online frequently surfaces these OUD mHealth websites due to their search engine optimization and advertising payments to appear in search. People seeking care then click on the website to learn about the services offered, answer screening questions, or enroll/pay for services. Paying for services through the website can avoid app store fees (i.e., "app store tax") thereby creating a business incentive to encourage visiting the website. Lastly, privacy policies for the apps and websites are hosted on the website. Therefore, websites are a critical component of OUD mHealth businesses.

To fulfill their promise of expanding access to quality care, virtual care platforms for OUD treatment and recovery should also meet or exceed the privacy and security standards for in-person care. By shining a light on these issues, we aim to urge legislators and other policy makers to take necessary measures to protect individuals who seek treatment and recovery support.

Appendix

SBIR & STTR Benefits

According to NIH¹⁶ “the SBIR and STTR programs are one of the largest sources of funding for early-stage companies in the United States. There are many benefits to securing SBIR or STTR funding, including:

- Funding is stable, predictable and not a loan.
- Capital is non-dilutive.
- Small businesses retain intellectual property rights.
- NIH’s rigorous peer-review provides recognition, validation and visibility to early-stage companies.”

Understanding SBIR/STTR Funding

Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs are US federal government grant and contract programs part of the America’s Seed Fund¹⁷ and US Small Business Administration (SBA). The SBIR/STTR program aims to stimulate technology innovation and foster/encourage diverse people participating in entrepreneurship.¹⁸ By design, SBIR/STTR is a means to providing seed funding to companies that may be too risky for private investors but have great potential.

Crucially, SBIR/STTR is an opportunity to obtain *non-dilutive funding* for early-stage research and development. Non-dilutive funding is appealing to early-stage companies because, unlike other start-up accelerators, non-dilutive funding does not include equity for the investment in the company.^{19,20} This means that these companies have more equity available for future funding rounds, founders, or employees which is attractive during hiring and when seeking additional investment. Additionally, SBIR/STTR companies retain ownership of any resulting intellectual property. Lastly, and as importantly, SBIR/STTR companies carry an implicit or even explicit “seal of approval” for their company from the federal government. This can appear on the company websites, advertising, investor decks, and press releases. Some companies are even highlighted in government blog posts.²¹ Prestige associated with the award can help attract more funding or support (e.g., venture capital, strategic partner).

¹⁶ <https://ncats.nih.gov/funding/small-business-programs/about>

¹⁷ <https://seed.nih.gov/>

¹⁸ <https://seed.nih.gov/women-owned>

¹⁹ <https://www.morganstanley.com/atwork/articles/what-is-equity-dilution?cid=mnsltwk-tl-sunrise-6091>

²⁰ <https://www.ycombinator.com/blog/dilution/>

²¹ <https://archives.nida.nih.gov/news-events/noras-blog/2019/10/nidas-help-startups-translate-addiction-science-new-technologies>

Understanding SBIR/STTR Grant Funding

Funding for SBIR/STTR grants is broken into phases based on how advanced the project is.

Small Business Program Phases	Description	\$
Phase I	The focus is on feasibility, technical merit, and commercial potential. A proof-of-concept.	\$295,924 over 24 months*
Phase II	A Phase II award is a continuation of the research and development efforts initiated in Phase I. Need a commercialization plan.	\$1,972,828 over 36 months*
Fast-Track	The fast-track process is both Phase I and Phase II in one application for review. This requires a fully developed Phase II application/plan at the time of submission.	
Direct to Phase II (SBIR Only)	If your project has already demonstrated feasibility but you have not received a Phase I SBIR or STTR, you can apply for a Direct to Phase II award and bypass Phase I.	
Phase III (non-NIDA funded)	Commercialization	

* 2023 numbers from: <https://nida.nih.gov/funding/small-business-innovation-research-sbir-technology-transfer-sttr-programs/about-sbir-sttr-programs/funding>

Understanding SBIR/STTR Grant Review and Decisions

NIH uses a dual peer review system consisting of non-NIH scientists (expertise in the applicant’s research area) and business professionals (backgrounds in commercialization of similar technologies) who evaluate SBIR/STTR applications. Evaluation criteria includes the value proposition, commercial opportunity, and their ability to scale for a *large societal impact*. The proposal “must have *sufficient technical details* for reviewers to understand the approach.”²² [emphasis added] Applications are evaluated based on significance, innovation, approach, investigators, and environment as described in the figure below.

Scored review criteria

- Significance** → Does the product address an important **problem**, and have commercial potential? Is there a market pull for the proposed product?
- Approach** → Are **design and methods** well-developed and appropriate? Are problem areas addressed? Are potential pitfalls and alternative approaches provided?
- Innovation** → How novel is the **technology/product** and the **approaches** proposed to test its feasibility?
- Investigator** → Are the investigators, collaborators, and consultants appropriately trained and **capable** of completing all project tasks?
- Environment** → Does the **scientific environment** contribute to the probability of success? **Facilities?** Independence?
- Commercialization** → Is the company’s **business strategy** one that has a high potential for success?

<https://doi.org/10.1016/B978-0-12-814926-3.00009-7>

New Regulations

The SBIR and STTR Extension Act of 2022 (September 30, 2022) requires Federal agencies to establish a due diligence program to assess *security* risks posed by applicants.²³ This is

²² <https://doi.org/10.1016/B978-0-12-814926-3.00009-7>

²³ <https://seed.nih.gov/small-business-funding/small-business-program-basics/foreign-disclosure-and-risk-management>

separate from the merit review described above. As part of this Act, there are also new (September 5, 2023) post-award monitoring and reporting requirements and recovery authority/repayment of funds from a company that either makes “material misstatement that NIH, CDC, FDA or ACL determine poses a risk to national security” or “there is a change in ownership, change in entity structure, or other substantial change in circumstances of the small business that NIH, CDC, FDA, or ACL determine poses a risk to national security.”²⁴

Information Related to NIDA SBIR/STTR Grants

NIDA has specific topics of interest: <https://nida.nih.gov/funding/small-business-innovation-research-sbir-technology-transfer-sttr-programs/about-sbir-sttr-programs/topics-of-interest>

And SBIR/STTR grants are searchable on <https://reporter.nih.gov/> or <https://reporter.nih.gov/search/jjKRM5Pc20S5JTnxjfsXtg/projects>

²⁴ <https://seed.nih.gov/small-business-funding/small-business-program-basics/foreign-disclosure-and-risk-management>