

How Digital Advertising Works in Healthcare Marketing

A guide about how advertising channels impact full funnel healthcare marketing, what data they capture from websites today, and the limited dataset they need to function.



Table of Contents

Why healthcare can't quit traditional digital advertising channels	3
Why privacy regulations could be a hit to digital advertising performance	4
Delivering high performance and privacy	4
How ad channels support the marketing funnel	5
How each advertising platform works	12
How to make advertising work in the context of privacy	24
Conclusion	33

Freshpaint

Why healthcare can't quit traditional digital advertising channels



50% of search starts on Google

(Source: Jumpshot 2019)

70% of US population on Facebook

(Source: Statista)



The healthcare industry spends over \$15B annually on digital advertising channels trying to reach consumers. No surprise here since consumers start 50% of their product searches on Google, and over 70% of the US population is on Facebook. Healthcare marketers are simply trying to meet consumers where they are by using digital advertising channels.



Why privacy regulations could be a hit to digital advertising performance

Digital advertising has evolved dramatically over the past decade, from manual pay-per-click models to highly targeted automated bidding algorithms powered by machine learning. This leads to a better return on investment from advertising, encouraging more spending on ads.

In practice, ad platforms can deliver more of the results healthcare organizations desire, like scheduled appointments or plan renewals.

For those automated bidding algorithms to work, healthcare organizations must send data back to advertising platforms, which use that data to fuel their high performance.

However, [new HIPAA privacy regulations](#) that dropped at the end of 2022, and were [updated on March 18, 2024](#), have presented a wrinkle. Abandoning advertising platforms where marketers can reach healthcare consumers isn't an option, and cutting off the data flow can tank performance.

Delivering high performance and privacy

The good news is that this is an opportunity for healthcare organizations to think strategically by reducing their security footprint while still delivering [high-performance digital advertising results](#). Throughout this guide, we'll discuss how each ad channel plays a role in reaching consumers, how those channels use data to work today, and how they can work in the context of a privacy-first healthcare marketing world.

Make Digital Ad Platforms High Performance & HIPAA-Compliant

[Learn more ↗](#)

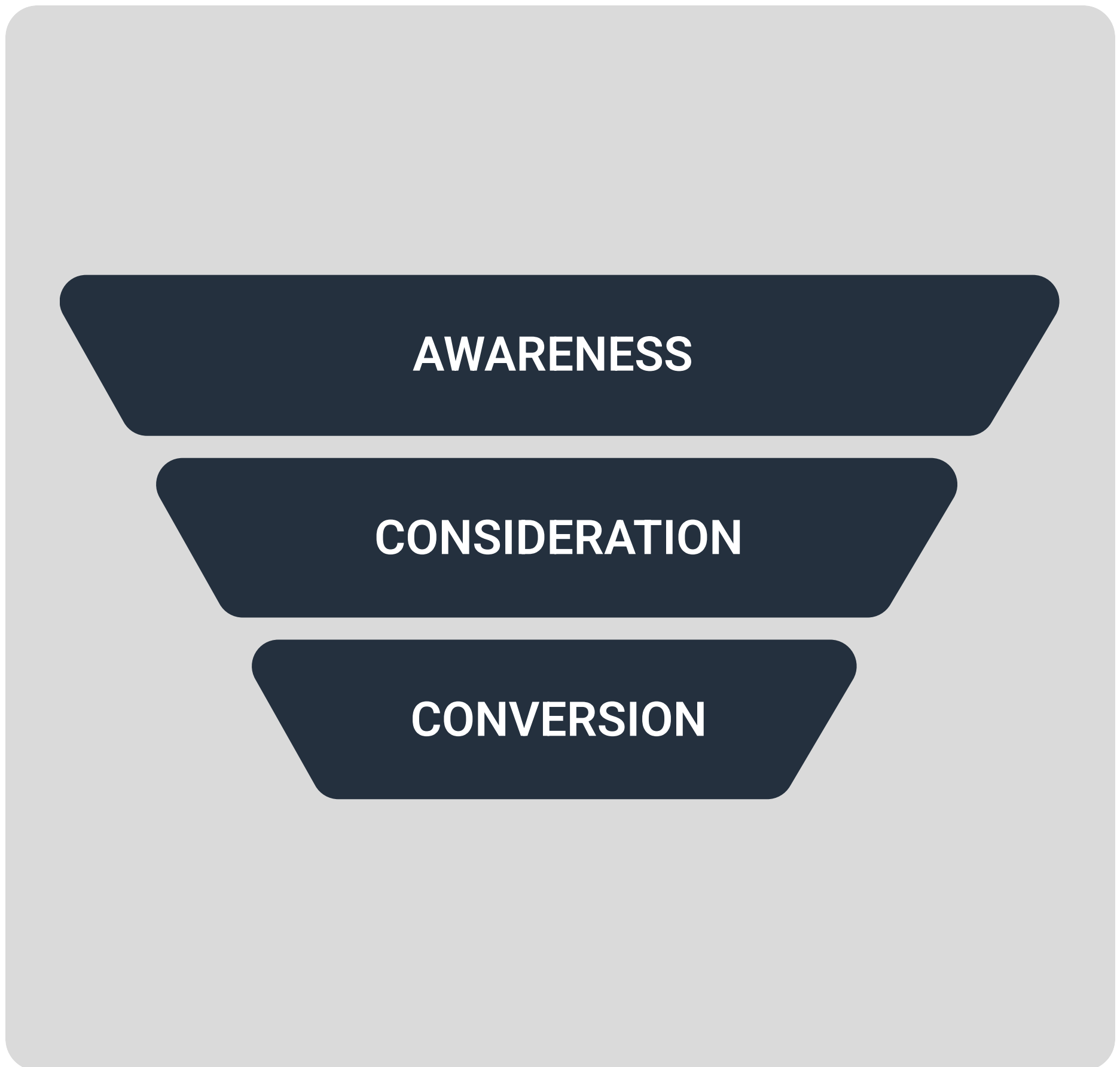
The diagram illustrates a data flow process. On the left, a laptop icon is labeled 'Your Website'. Two arrows point from the laptop to a central box containing a bar chart and a checkmark. From this central box, three dashed lines connect to circular icons for Facebook, Google Ads, and Microsoft Advertising, representing data being shared with these platforms.



How ad channels support the marketing funnel

Before we get into each advertising platform, let's cover how healthcare marketers leverage each tactic to build a marketing strategy that reaches the consumers in their market.

Each digital marketing platform and tactic plays a role in the individual stages of a consumer's journey. We'll start by breaking down the funnel and then get into how each advertising tactic fits into that stage.





Awareness

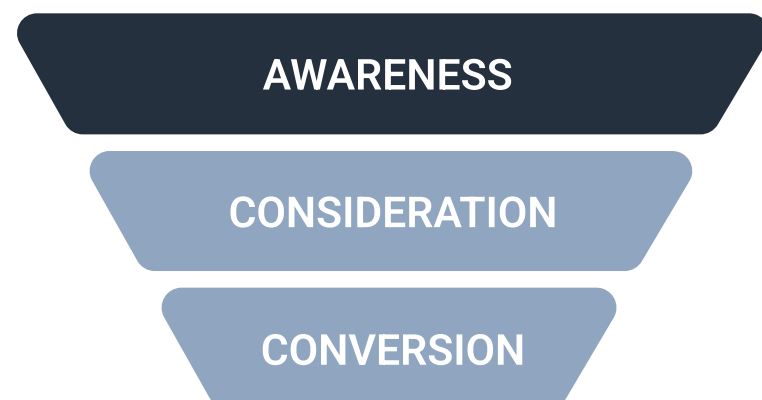
Awareness is critical to introducing a healthcare brand's areas of expertise to consumers.

For example, consider an urban healthcare center known nationally for its cancer treatment capabilities. Given the widespread impact of cancer, raising awareness about this specific expertise can spark recognition among consumers. This recognition may come into play when they, or someone they know, require care in the future.

How do healthcare marketers leverage advertising channels to promote awareness of brands and services?

Programmatic advertising

Marketers, or their agency partners, typically use demand-side platforms (DSPs) like StackAdapt, TradeDesk, and Basis to buy ad space across the Internet to reach their target audience. This can include mobile, banner, and video ads like those pictured below.



Example of a display ad served on a programmatic advertising platform

DSPs offer the advantage of buying all programmatic advertising on one platform and offering a higher level of personalized targeting to ensure marketers can reach their desired audience.

Linear TV

Linear TV is traditional television. And it still earns a whopping \$60B in annual advertising spend (Source: eMarketer 2023).

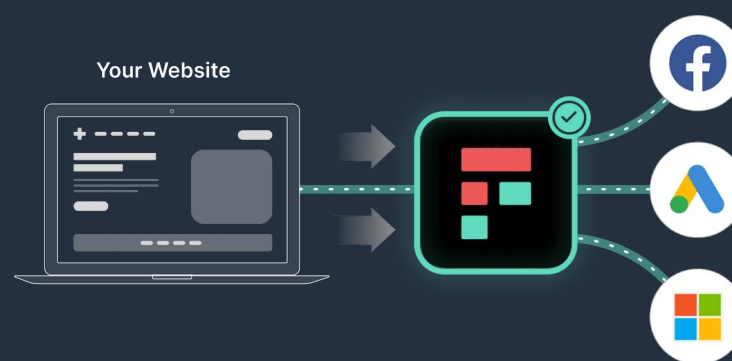
Traditional TV has some strong use cases, like reaching a broad audience simultaneously during a live event like the Grammys or in its ability to reach older audiences. Roughly 38% of audiences 55 or older watch traditional TV (Source: Tech Report 2023).

Traditional TV's significant disadvantages are its lack of analytics, the ability to skip commercials, and rapidly shrinking viewership.



Make Digital Ad Platforms High Performance & HIPAA-Compliant

[Learn more ↗](#)



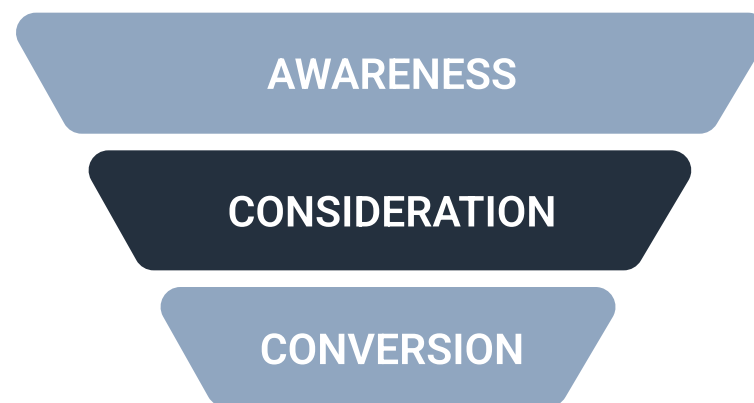
Connected TV

While traditional TV viewership is dropping, connected TV (CTV) continues to gain a larger share of ad spending. Projected to grow from \$25B to \$40B in 2027, CTV delivers the high engagement of traditional TV with the targeting and analytics of digital advertising.

Marketers can leverage CTV platforms like Madhivie and Mountain to provide highly targeted ads that experience high video completion rates and can get detailed metrics in real-time.

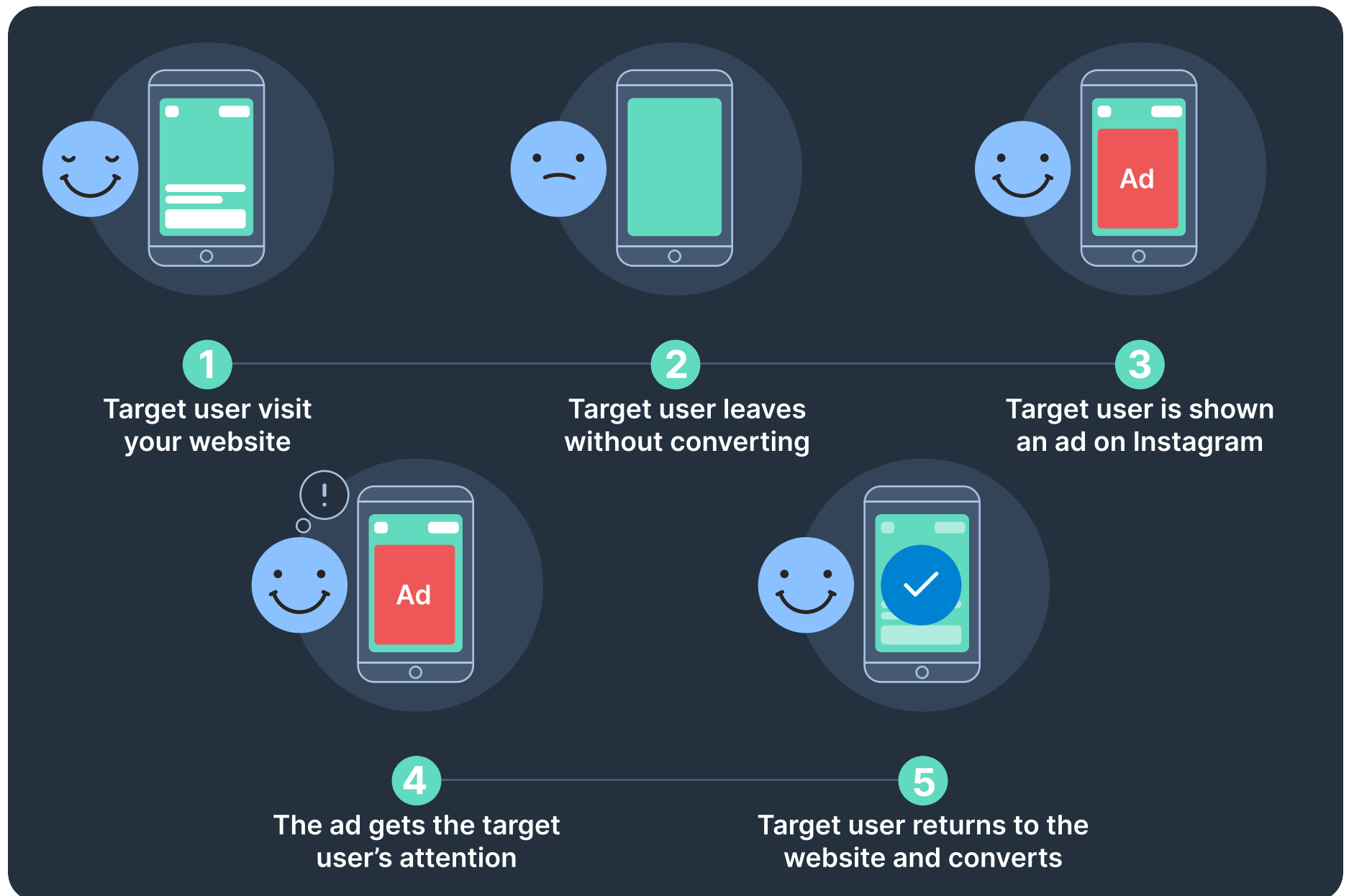
Consideration

In the consideration stage, the consumer has been made aware of the problem, and now it's time to begin introducing solutions and services that address it. For instance, consider a person who has experienced a skiing injury and suspects they need to see a doctor about their knee injury. A healthcare organization might introduce a new range of repair-based solutions aimed at preserving the meniscus in the knee, instead of removing the damaged part.



Retargeting

Retargeting is a cost-effective form of advertising that moves consumers further along their journey with a healthcare brand once they have awareness. Digital ads target users previously engaged with a healthcare website, landing page, or social media presence.



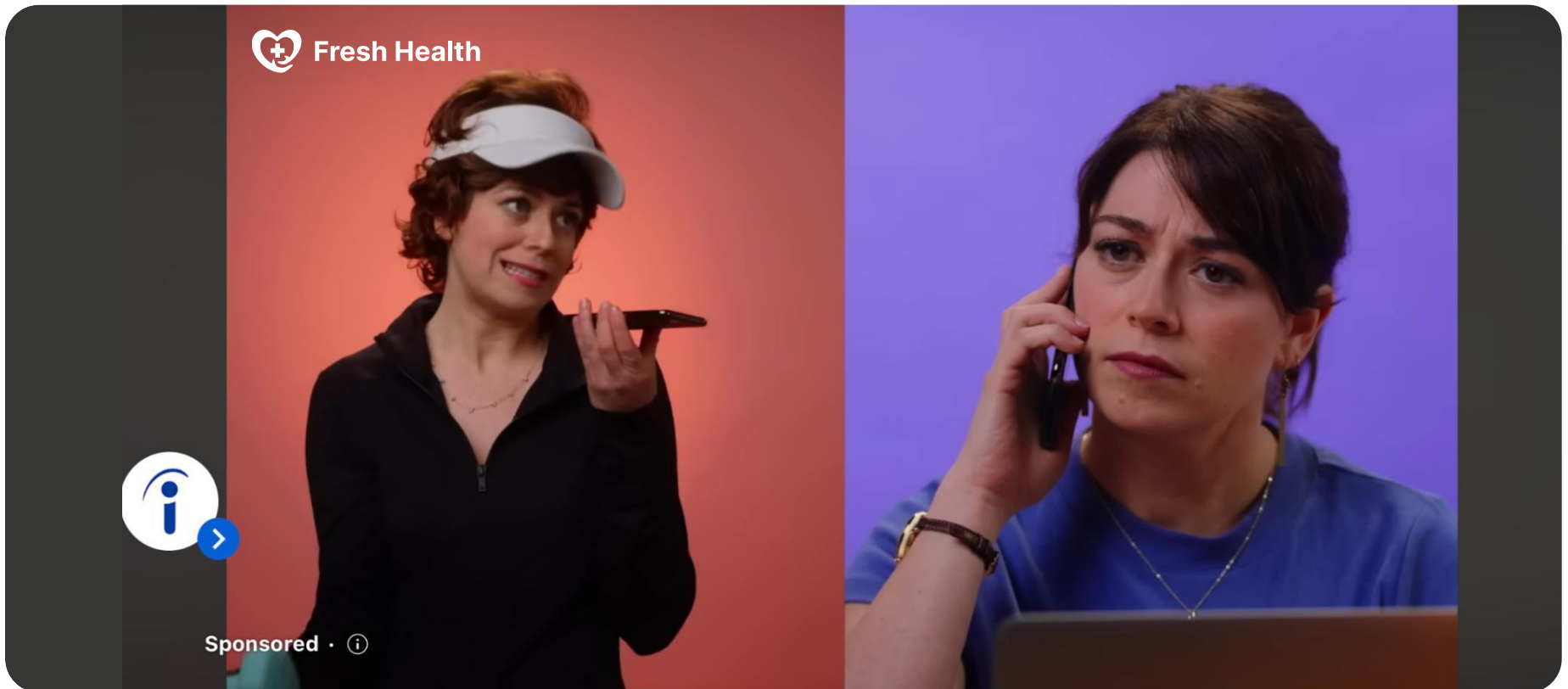
How retargeting works to re engage consumers

For example, a consumer may have visited a healthcare website multiple times without scheduling an appointment or taking some desired action. Marketers can serve that same user ads to recapture their attention and bring them back to the website to capture the scheduled appointment.

Video

Video advertising inserts promotional content before, during, or after streaming content. YouTube pre- and mid-roll video ads are among the most popular formats, but social media platforms and mobile apps also support this advertising asset.

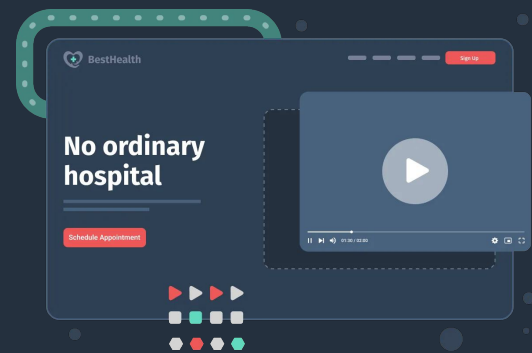
Video ads can be impactful in the consideration phase because the format provides an opportunity to tell more of the healthcare brand story in a richer format.



Example of a video ad in YouTube

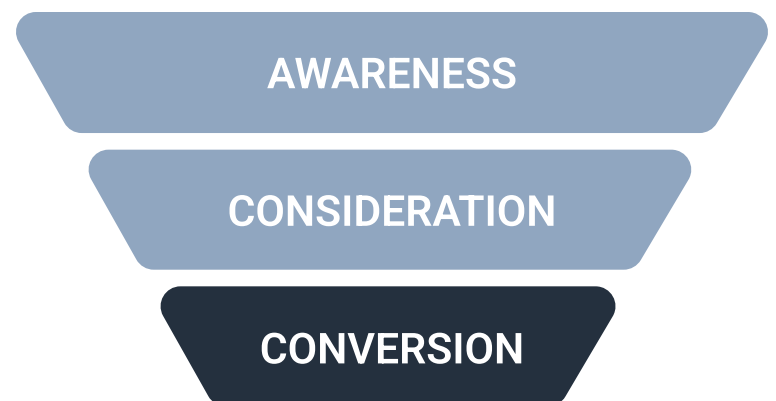
Improve Visitor Experience with HIPAA-Compliant Embedded Video

[Learn more ↗](#)



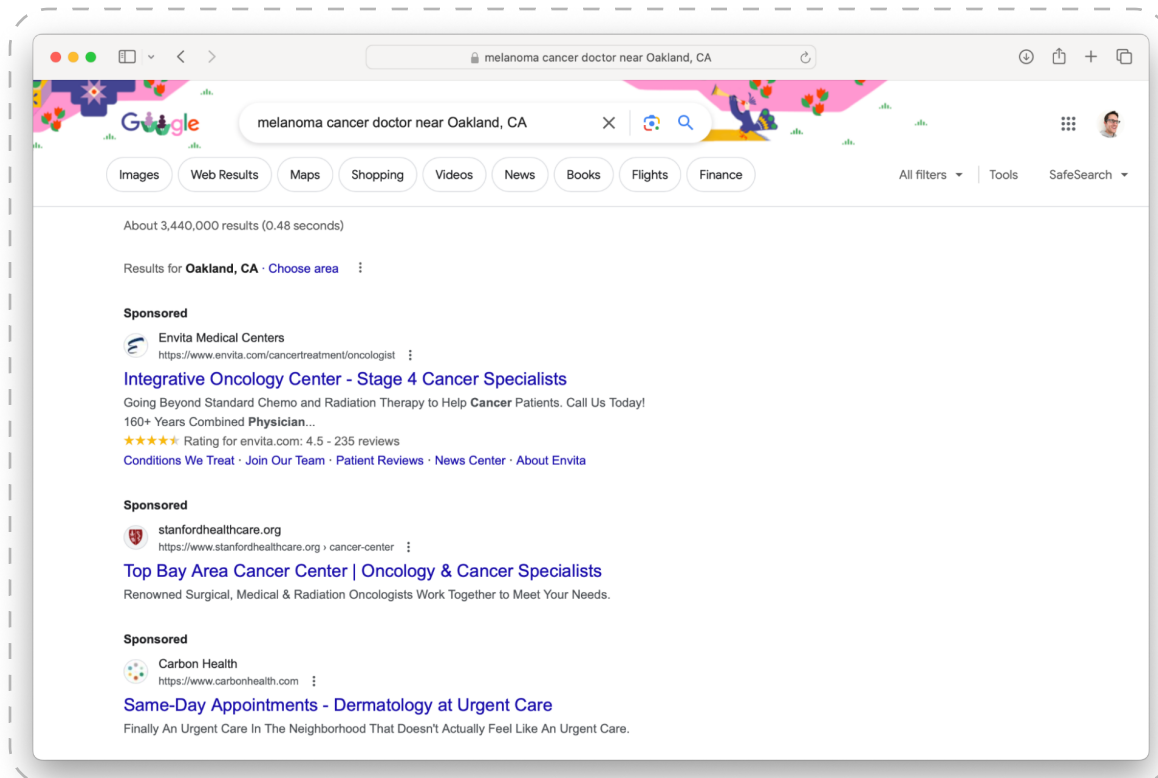
Conversion

Most people think this is the ONLY thing marketing does: convert consumers to buyers—or at least convert those consumers to scheduled appointments. This stage yields the most desired results and is the most measurable. The fruits of this demand capture stage are often the results of the labor in the Awareness and Consideration stage.



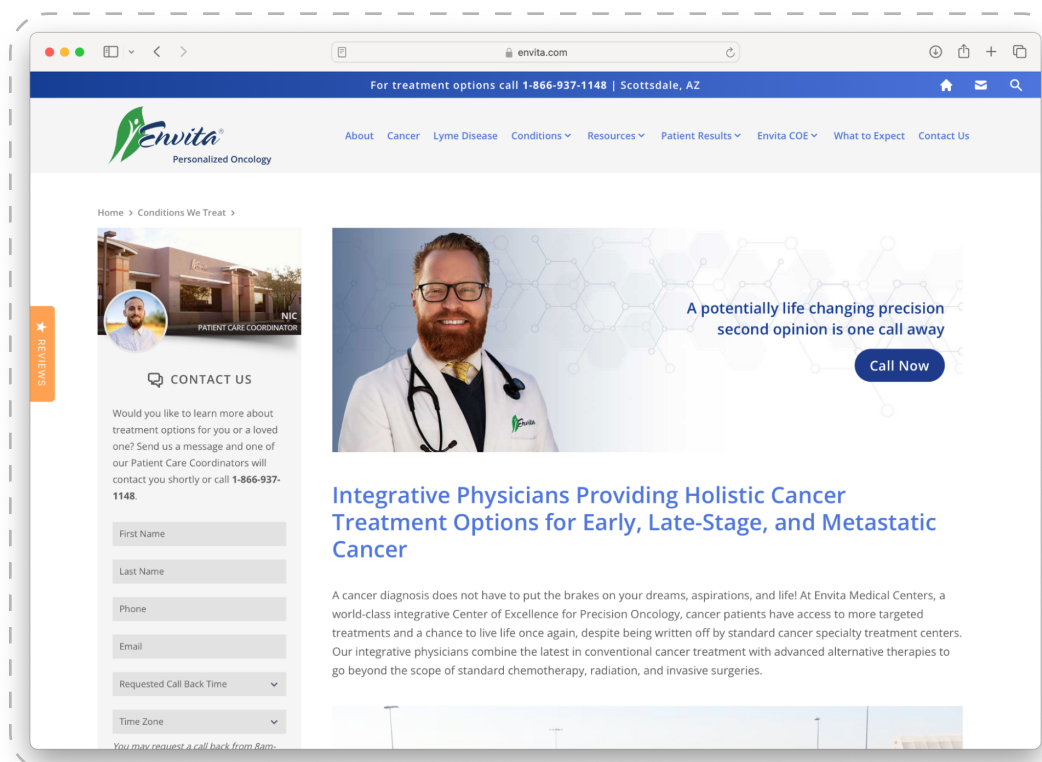
Search Engine Marketing

The most powerful advertising channel ever created answers the questions of healthcare consumers and takes them straight to solutions for their problems. For a leading cancer treatment center, search advertising platforms like Google Ads and Microsoft Ads take consumer queries like "melanoma cancer doctor" and allow them to seek specialized care with an expert.



A Google search query and its sponsored results

This straight-from query to booked appointment is a win for both the consumer and the healthcare organization.



An example of a landing page designed to capture future patient conversions from a search ad click

For marketers, one of the reasons search engine marketing is so popular is that it's also highly measurable. Since the intention is to capture a high-intent query, serve a helpful ad, and then capture a high-value conversion like a booked appointment, it's straightforward to tell whether ads are effective.

Most organizations will continue scaling their spending in this advertising area if the return on investment exists.

Direct Response Advertising

Direct response advertising platforms, such as Facebook Ads and TikTok, use the interests and demographic information available within their platforms to target a specific audience. These platforms display visual ads directly in the user's feed to grab their attention and motivate them to take a specific action, such as scheduling an appointment.

Say a marketer works for a women's healthcare brand, and they know something about their most valuable consumers' age, income level, and interest. That marketer could build a specific audience using Facebook's in-platform audience-building tools to improve the effectiveness of their advertising.

Advantage+ audience ⁺

Our ad technology automatically finds your audience. If you share an audience suggestion, we'll prioritize audiences matching this profile before searching more widely. [Learn more](#)

Custom audiences Create new ▼

Age

25 ▼ 45 ▼

Gender

All Men Women

Detailed targeting

Include people who match ⓘ

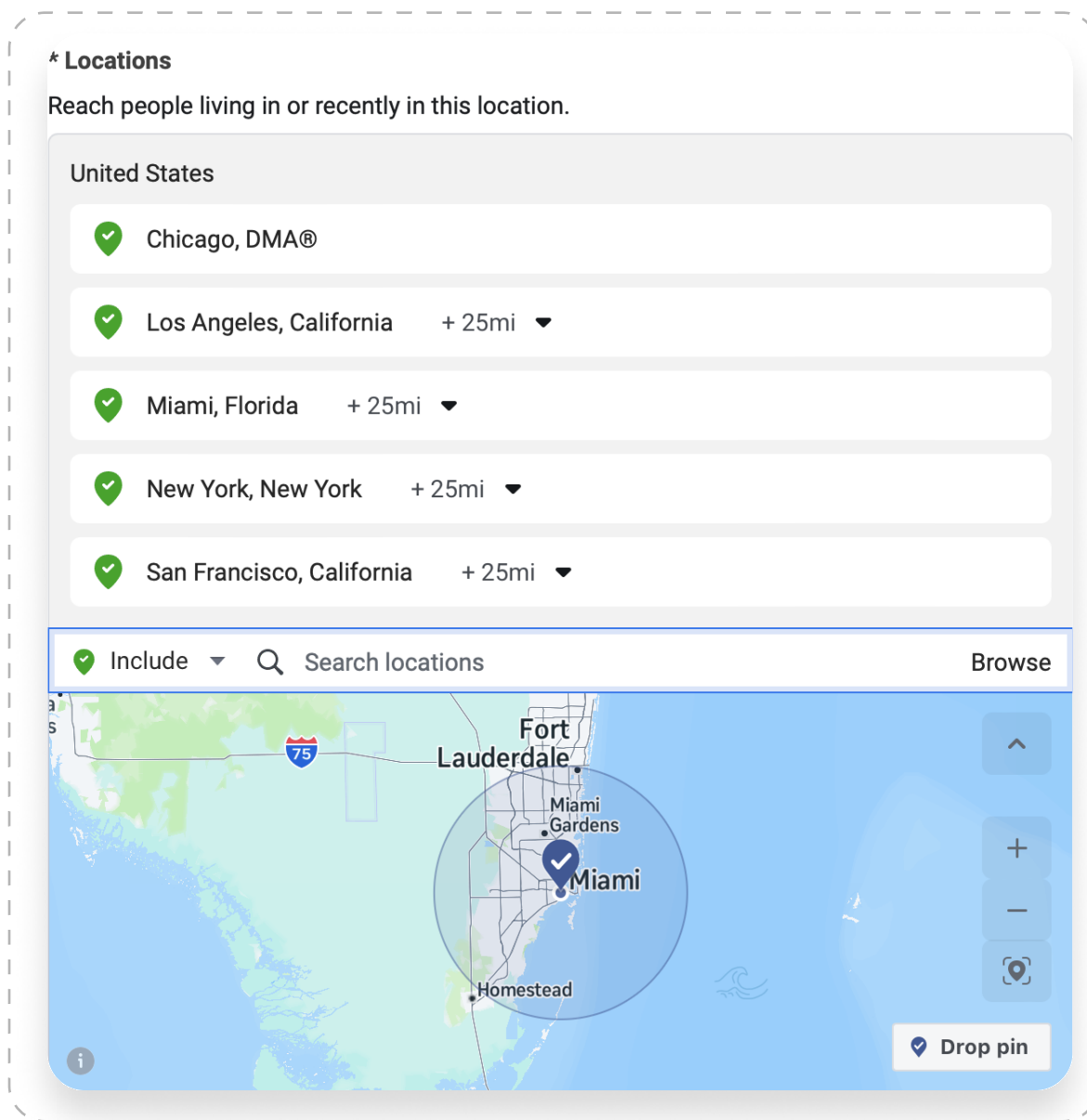
[Interests](#) > [Additional interests](#)

Running club (club)

Trail running (running)

Suggestions Browse

Narrow Audience



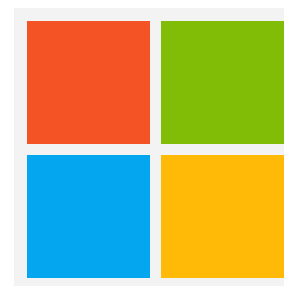
How each advertising platform works

Search Engine Marketing

Major Platforms



Google Ads



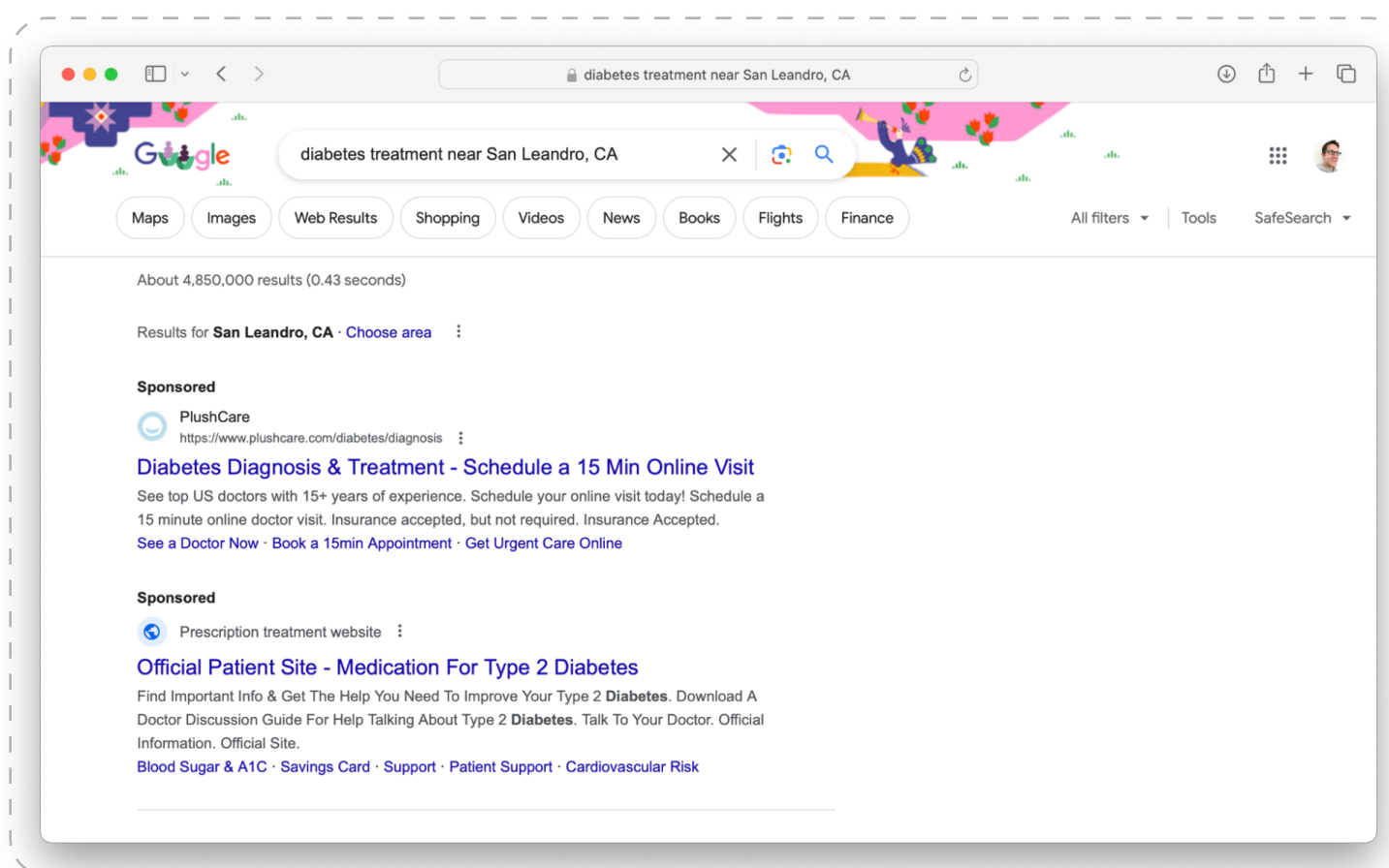
Microsoft Ads

Goal

Turn a consumer's query into an actual conversion, like a scheduled appointment or a new insurance plan subscriber.

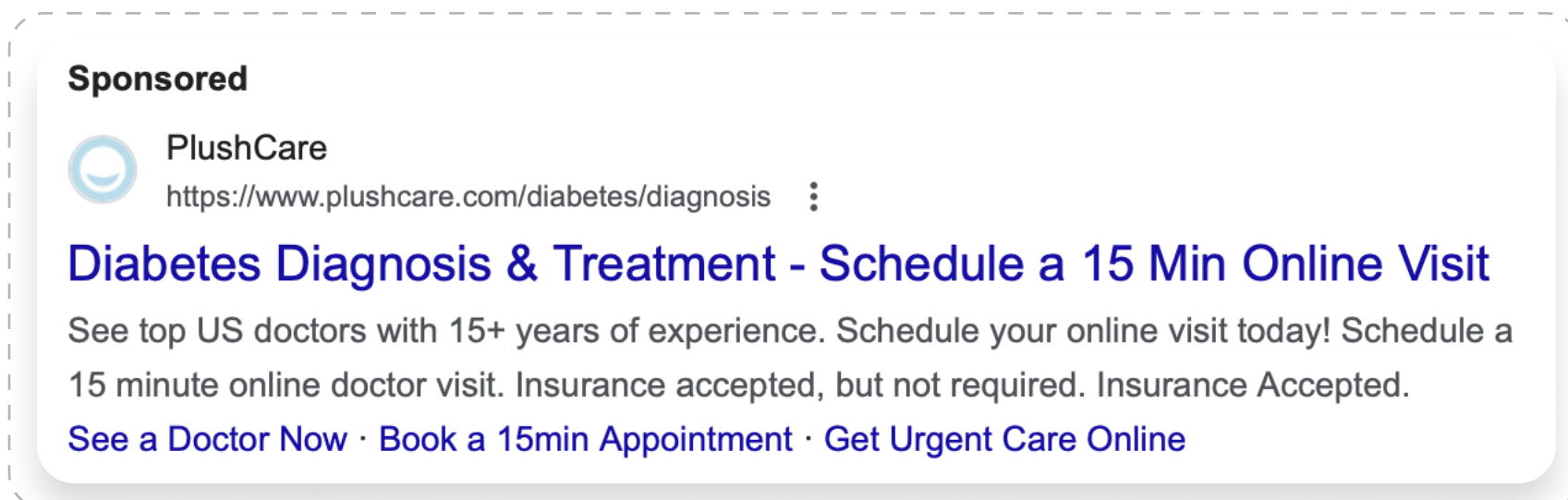
Audience

Marketers create audiences on the ad platform, not based on interactions with the healthcare website. Consumers type a query ("diabetes type 2 treatment") in the search engine platform, and using automated bidding strategies behind the scenes, the search platform posts sponsored results in real-time. If an advertiser is willing to pay, they can have their results consistently land at the top of the page.



Ad Creative

The ad creative is a text-based ad created in the ad platform.

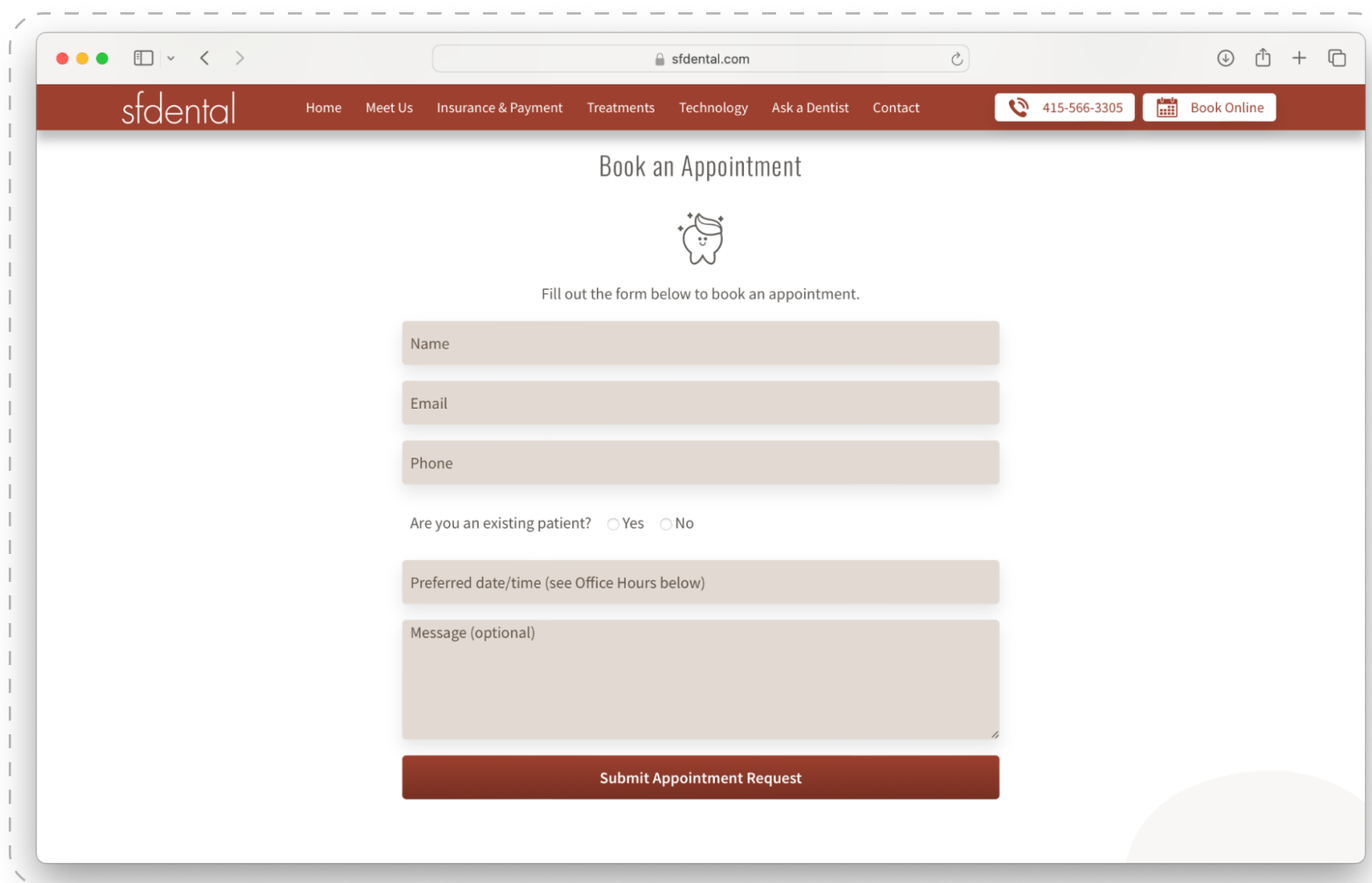


Data Sharing

Traditionally, a tracking pixel from the advertising platform is installed on the healthcare website. This pixel sends data about user actions back to the platform, helping it target ads better in the future.

Let's say scheduled appointments are the primary goal of a national dental service organization when running search ads on Google. Maybe their marketing team decides that "cosmetic dentistry" and "dental exam" are keywords worth bidding on, so they set up campaigns and ads for those keywords.

They also set up a landing page to capture those clicks and turn them into scheduled appointments.

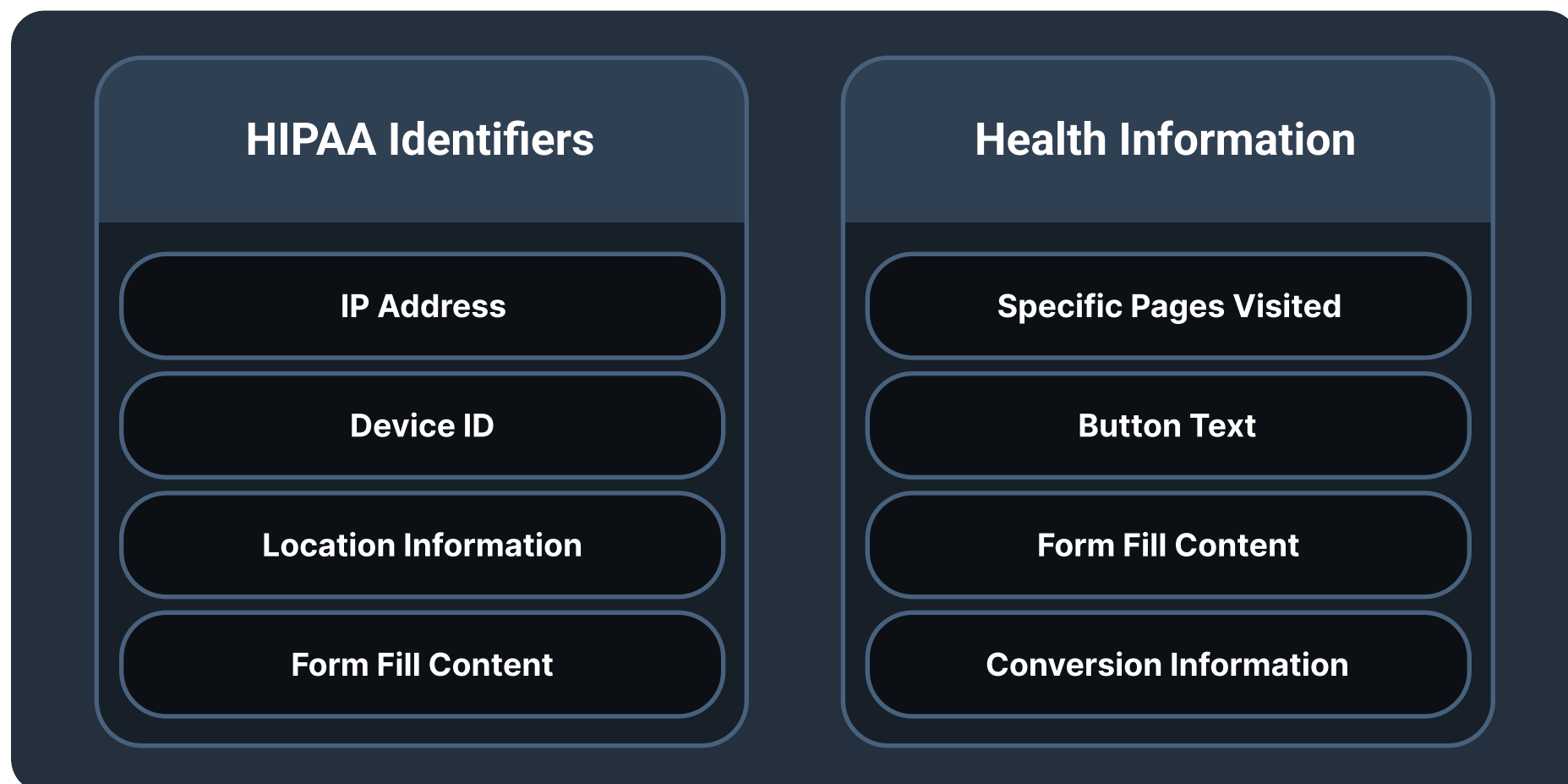


The image shows a screenshot of a web browser displaying the 'Book an Appointment' form on the website sfdental.com. The browser's address bar shows the URL 'sfdental.com'. The website's navigation menu includes 'Home', 'Meet Us', 'Insurance & Payment', 'Treatments', 'Technology', 'Ask a Dentist', and 'Contact'. There are also contact details: a phone number '415-566-3305' and a 'Book Online' button. The form itself is titled 'Book an Appointment' and features a small tooth icon. Below the title, it says 'Fill out the form below to book an appointment.' The form fields include: 'Name', 'Email', 'Phone', a radio button question 'Are you an existing patient?' with 'Yes' and 'No' options, 'Preferred date/time (see Office Hours below)', and a 'Message (optional)' text area. A red 'Submit Appointment Request' button is at the bottom of the form.

Search ad platforms use those initial successful conversions to improve their future targeting. The native tracking pixel feeds Google data about the first 50 converted consumers. Since Google has been collecting data points about each of those consumers for as long as they've been on the Internet, they can find things those first 50 consumers have in common.

When someone searches "cosmetic dentistry" in the future, Google will optimize by only serving ads to the consumers they think share commonalities with those who have already converted. This perfectly matches the marketer's goal of only serving ads to consumers most likely to schedule an appointment.

However, privacy regulations cause problems for healthcare marketers because [search ad platforms like Google](#) and Microsoft collect a lot of data that could violate patient privacy. When a consumer visits a healthcare website, the ad platform's pixel loads on the consumer's computer, gaining access to a lot of sensitive information, such as:



The Office for Civil Rights (OCR) stated in its [March 18, 2024 update](#) that sharing any combination of HIPAA identifiers and health information from a healthcare website's unauthorized pages to web tracking technologies without a proper agreement (BAA) violates HIPAA rules.

“If an individual were looking at a hospital’s webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual’s IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual’s health or future health care.”

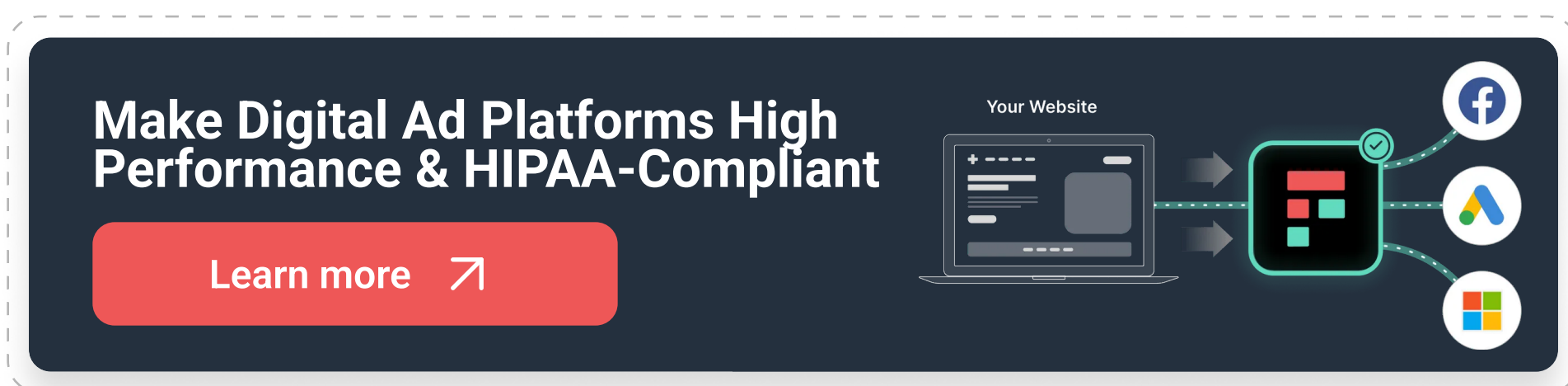
Google and Microsoft only need some of this data to perform their job, but they want to collect it anyway because it improves the future growth of their ad businesses.

Risk Summary

Using Google or Microsoft Ads isn't a risk in itself since neither platform is covered by HIPAA. A consumer searches and interacts with ads on a platform that is not a covered entity.

The risk lies when the consumer clicks on an ad and is directed to the healthcare website. The native tracking pixel collects and shares information about that consumer that could be considered [protected health information](#) (PHI). The free flow of data shared by the search ad platform's pixel puts healthcare organizations at risk.

No search engine marketing platforms will sign a [business associate agreement](#) (BAA).



Make Digital Ad Platforms High Performance & HIPAA-Compliant

[Learn more](#) ↗

Your Website

Facebook, Google Ads, Microsoft Ads

Direct Response Advertising

Major Platforms



Goal

Turn interest-based ads in a consumer's feed into actual conversions, such as a scheduled appointment or a new insurance plan subscriber.

Audience

The audience is created on the ad platform and is not based on interactions with the healthcare website.

Advantage+ audience ✦

Our ad technology automatically finds your audience. If you share an audience suggestion, we'll prioritize audiences matching this profile before searching more widely. [Learn more](#)

Custom audiences Create new ▼

🔍 Search existing audiences

Age

25 ▼ 45 ▼

Gender

All Men Women

Detailed targeting

Include people who match ⓘ

[Interests](#) > [Additional interests](#)

Running club (club)


Trail running (running)

🔍 Add demographics, interests or behaviors Suggestions Browse

Narrow Audience

Ad Creative

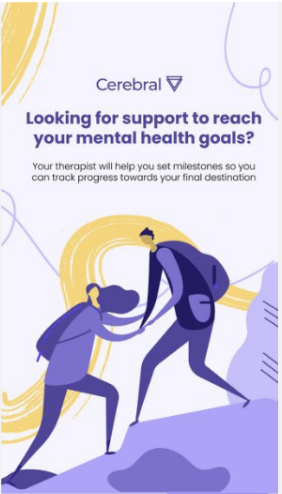
Ad creative combines visuals and text created in the ad platform.



Cerebral

Sponsored

Discover Cerebral Way: our new personalized path to mental wellness. Start your journey today!



Cerebral
Looking for support to reach your mental health goals?
Your therapist will help you set milestones so you can track progress towards your final destination

[GET.CEREBRAL.COM](https://get.cerebral.com)
[Your Personalized Path to Feeling Better](#)

Sign Up

Data Sharing

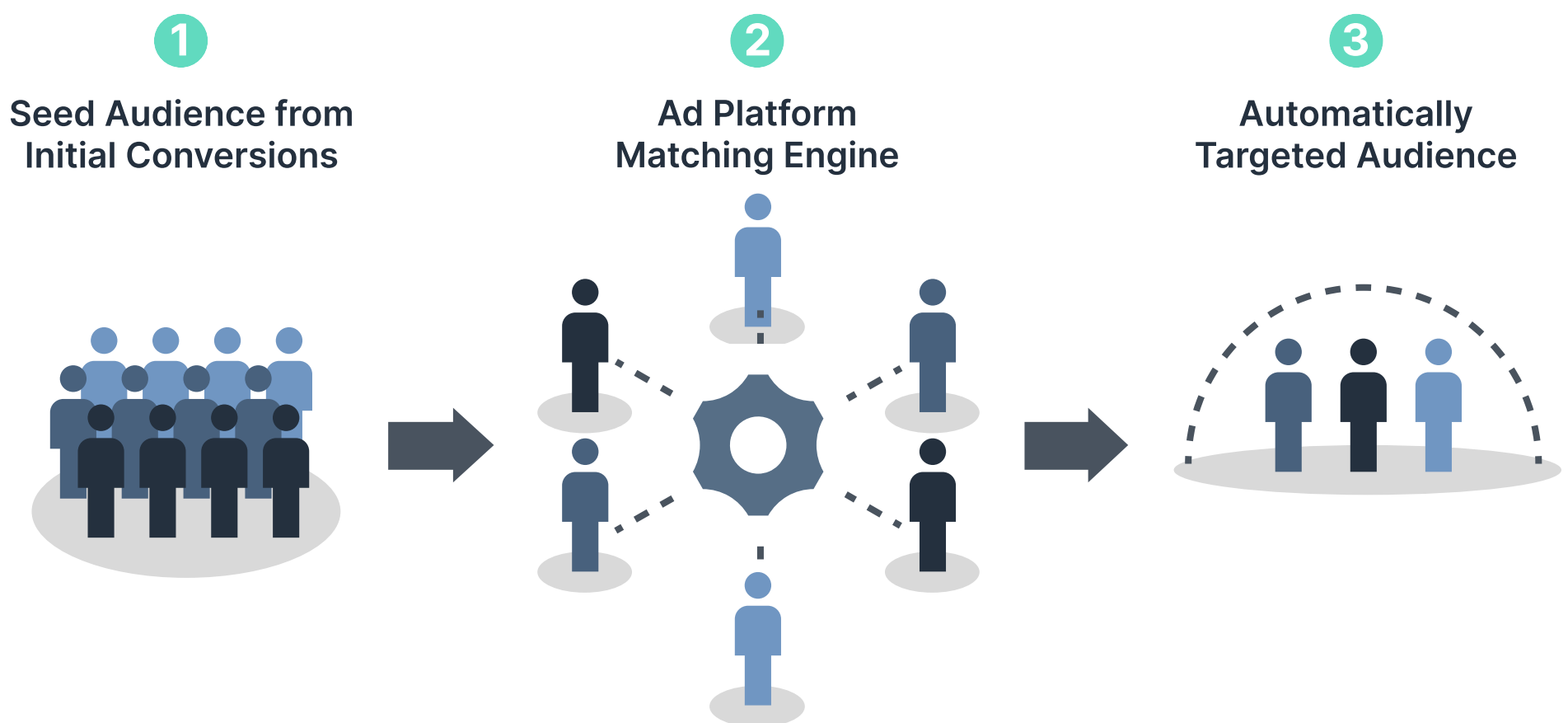
Traditionally, the ad platform's native pixel is installed on the healthcare website to feed back data about conversions so the direct response ad platform can optimize targeting to improve future results.

A national healthcare organization specializes in podiatry services for runners. It wants to run campaigns in regions where it thinks it has the best target audience. The campaign aims to get consumers to schedule a custom orthotics consultation appointment. Marketers can build that audience directly on an ad platform like Facebook.

Like search ad platforms, direct response advertising platforms use those initial successful conversions to improve their targeting in the future. The native tracking pixel feeds Facebook data about the first 50 converted consumers.

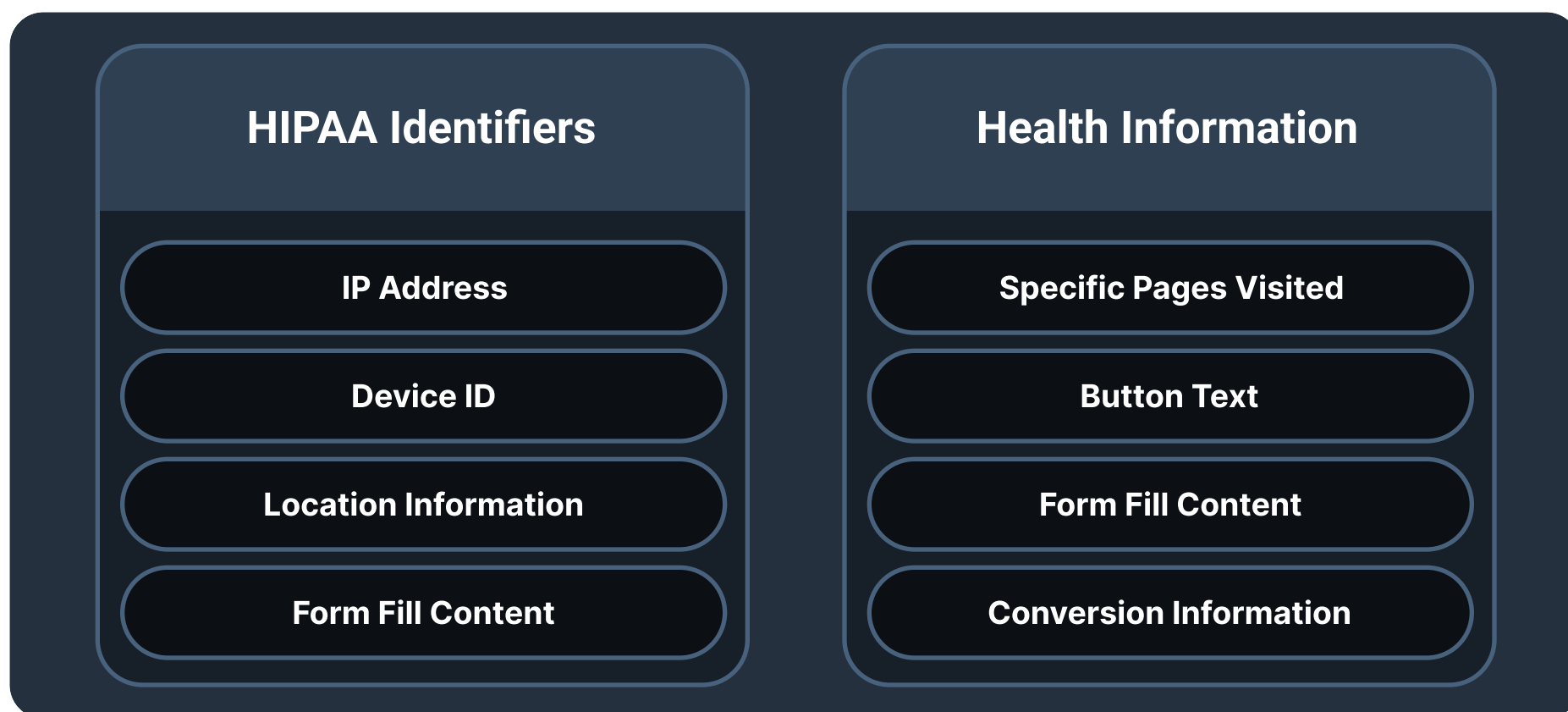
Since Facebook has collected data points about each of those consumers for as long as they've been using the social media platform, they can determine a lot about what those first 50 consumers have in common.

Facebook can automatically expand its audience targeting to find more consumers on its platform who it thinks will schedule that custom orthotics appointment. Given enough data, platforms like Facebook are incredibly effective at only serving ads to audiences most likely to convert.



However, privacy regulations cause problems for healthcare marketers because direct-response advertising platforms [like Facebook](#) and TikTok collect a lot of data that could violate patient privacy.

When a consumer visits a healthcare website, the ad platform's pixel loads on the consumer's computer, gaining access to a lot of sensitive information, such as:



Facebook, TikTok, and X only need some of this data to perform their job, but they want to collect it anyway because it improves their ad business.

No direct response ad platforms will sign a business associate agreement.

Risk

Creating and serving consumer ads on a direct-response advertising platform like Facebook or TikTok isn't a HIPAA violation in itself. These platforms aren't covered by HIPAA. Consumers willingly log into these platforms to interact with organic feeds and the ads within them.

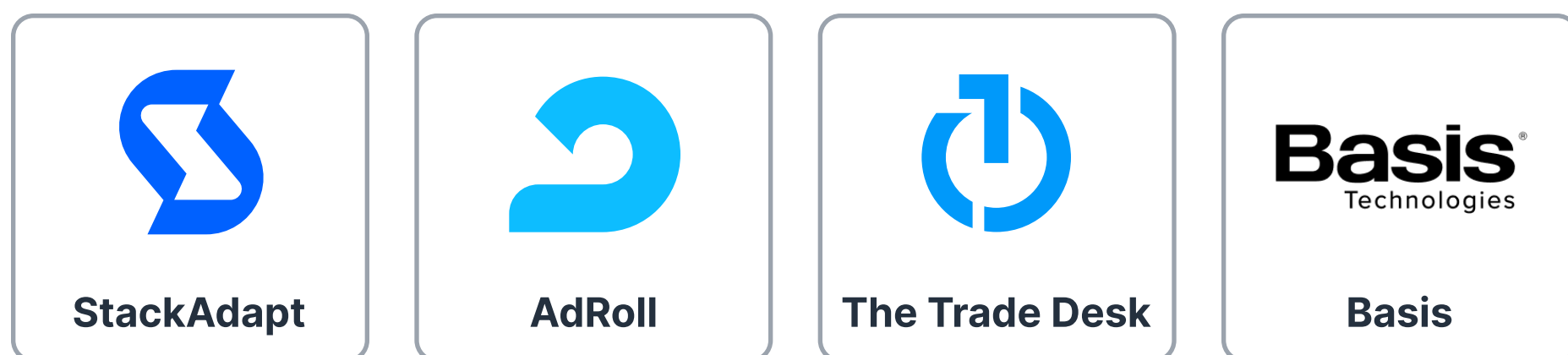
The risk lies when the consumer clicks on an ad and is directed to the healthcare website. The native tracking pixel collects and shares information about that consumer that could be considered protected health information. The free flow of data shared by the ad platform's pixel puts healthcare organizations at risk.

No direct response advertising platforms will sign a business associate agreement.

A video player interface with a dark blue background. On the left, the text 'Baptist Health's Journey to HIPAA-Compliant Digital Marketing' is displayed in white. Below it is a red button with the text 'Read the Story' and a white arrow icon. On the right, there is a video thumbnail showing a woman with glasses smiling. Below the thumbnail is the Baptist Health logo and a red play button icon.

Programmatic Advertising

Demand-side platforms like StackAdapt, AdRoll, The Trade Desk, and Basis allow marketers to buy ads.



Goal

Programmatic advertising uses automated bidding to buy up digital ad space on the web, mobile apps, video, and social media to help create awareness of a brand and its services. Audience

Audience

Audiences can be created in several ways: the programmatic ad platform's proprietary dataset, third-party datasets (owned by some other ad platform), or a healthcare organization's first-party data (data about visitors to the healthcare organization's website).

Ad Creative

Ad creative is highly visual and limited in text. Many ad platforms restrict the percentage of the ad that can contain text. These ads can be dynamic and created within the ad platform or created offline and uploaded to the ad platform.





Data Sharing

Programmatic ad platforms rely on third-party cookies and tracking pixels to measure the effectiveness of their advertising campaigns.

When a consumer views or interacts with an advertisement, the pixel adds a third-party cookie to the consumer's browser. That third-party cookie identifies the user and can indicate whether the consumer clicked or viewed the ad.

Unlike search ads and direct response ads, programmatic advertising relies on display ads that are less likely to be clicked on. This is where view-through conversions (VTCs) are essential. If the consumer viewed the ad but didn't click and converted later, the third-party cookie can measure that as a VTC.

Marketers don't expect a display ad to result in a click-to-conversion, but they expect consumers who see them to eventually convert.

The third-party cookie tracks a consumer's general web browsing behavior. For example, browsing a healthcare provider's website (the ultimate destination for any successful advertising campaign) could inevitably include health information. The third-party cookie also intercepts data that identifies a particular consumer.

Combining the two results in protected health information being shared with ad platforms that don't sign business associate agreements.

Risk

Using a programmatic advertising platform to create awareness with healthcare consumers can be risky when you utilize native pixels, third-party cookies, and first-party data to build audiences.

Third-party cookies rely on sharing information about a consumer's interaction with a healthcare website, which could be considered protected health information. The free flow of data captured and shared by those third-party cookies puts healthcare organizations at risk.

Additionally, programmatic platforms can leverage a healthcare organization's first-party data to build audiences. For example, organizations may want to take their highest-value patients, upload them to a programmatic platform, and use machine learning to create lookalike audiences to reach the broader market.

Depending on the dataset required to upload, this could be high risk, and it is precisely [what the FTC and HHS have been cracking down on](#).

None of the major programmatic advertising platforms sign a business associate agreement.

Retargeting

Major Platforms



Goal

Re-engaging visitors to your site that didn't initially convert is one of the most common reasons to do retargeting. However, it can also be used to create personalized experiences or retain existing patients.

Audience

Retargeting relies on leveraging consumers' previous interactions on a healthcare website. For example, you might want to retarget people who visited a page to choose a healthcare insurance plan but never selected one.

Retargeting could present legal risks since the healthcare organization would provide that audience and contain HIPAA identifiers and potential context about the consumer journey on that healthcare site.

Ad Creative

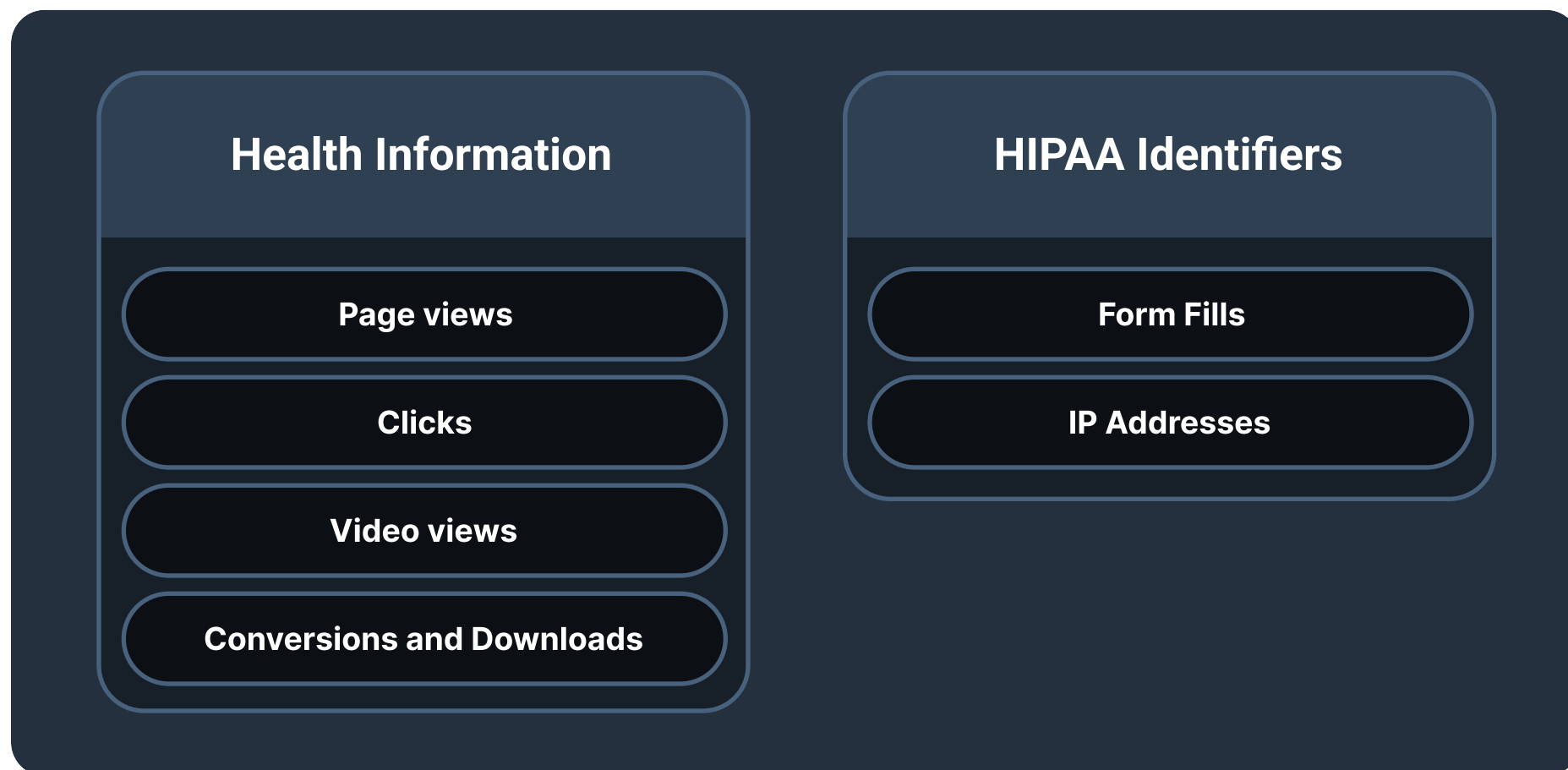
Retargeting is typically most effective when the ad is related to where someone left off in their journey. For example, if a potential patient didn't schedule an appointment, serving them an ad with relevant creative might work to get them to convert, but it could also introduce health context.

Data Sharing

Retargeting works similarly to demand-side platforms. Tracking pixels on your site can apply a cookie to each consumer's browser when they visit a healthcare website. That cookie can use the IP address to recognize that consumer when they visit other websites where retargeting ads could be served.



In addition to IP addresses, retargeting tracking pixels can capture other data points from a healthcare organization's website that could be considered HIPAA identifiers and health information:



Risk

Using native tracking pixels for retargeting platforms presents a high risk regarding privacy. That's because the cookies they place will likely capture both HIPAA identifiers and health context, sharing protected health information with ad platforms that do not have a business associate agreement as an option.

Additionally, because retargeting platforms rely on an audience provided by the healthcare organization, the context of the audience itself and the ad creative could potentially introduce protected health information. That's because serving a diabetes ad to an audience that interacted with content about diabetes treatment could make it easy to infer that everyone receiving that ad might be seeking diabetes treatment.

Get a HIPAA Risk Assessment

[Scan your website ↗](#)

Tracking Tools (10)			
Tracking tool	Pages detected	Risk	First detected
Google Analytics	6	HIGH RISK	11/1/2023 →
YouTube	5	HIGH RISK	11/1/2023 →
Google Fonts	127	LOW RISK	11/1/2023 →

How to make advertising work in the context of privacy

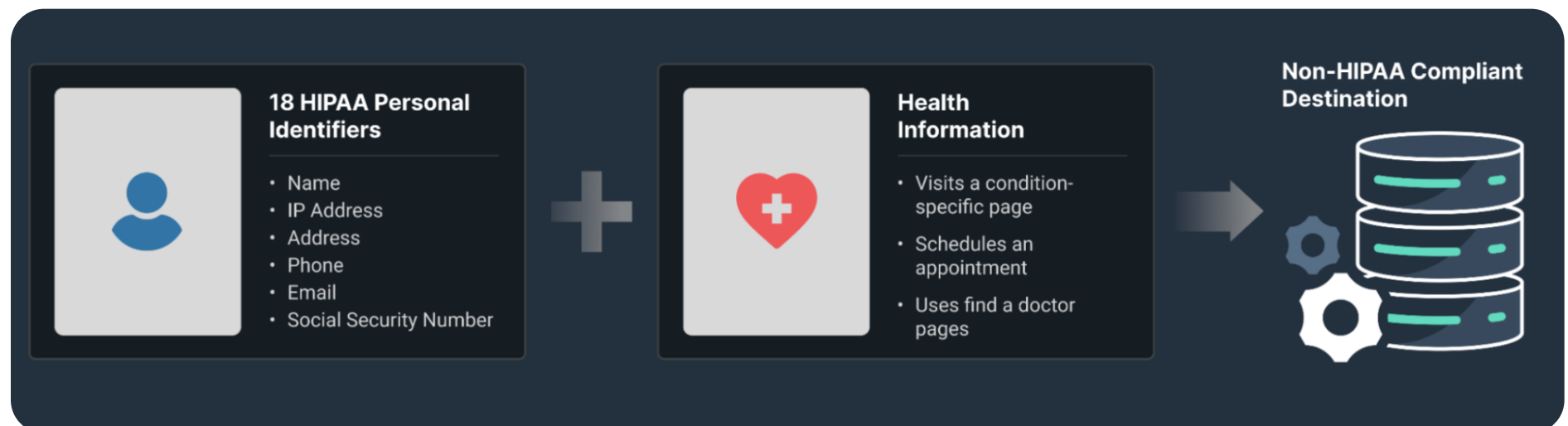
As a healthcare organization collaborates and decides to achieve high-performance marketing in a privacy-first way, there are two significant considerations—risk tolerance and how they interpret [the most recent HIPAA guidance](#) around sharing protected health information.

Let's start by interpreting the guidance. HHS was clear that protected health information on unauthenticated pages like a website is the combination of HIPAA identifiers and health information, as pictured below.

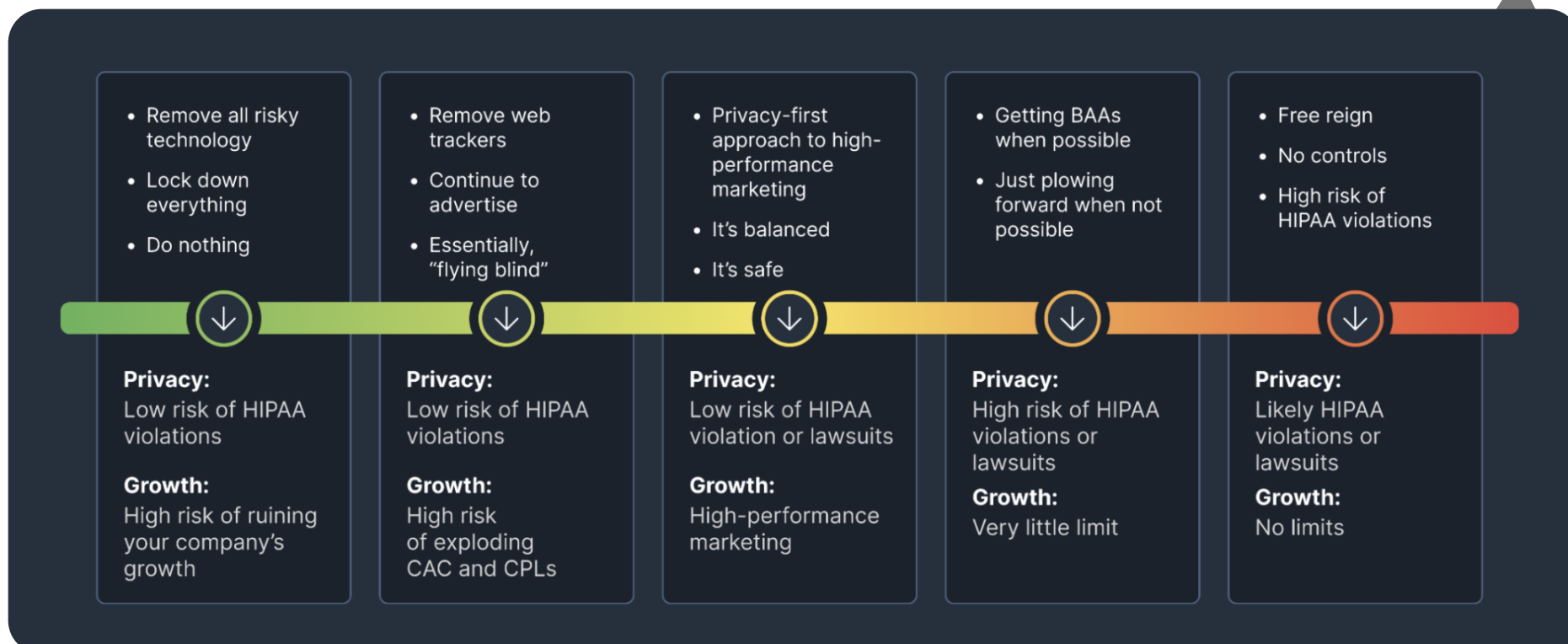
We interviewed privacy partner Dori Cain at Faegre Drinker to get her take. In Dori's interpretation, she explains that PHI is any individually identifiable information about a person's past, present, or future physical or mental health condition, provision of healthcare, or past, present, or future payment of health care.

“So here, you're really looking at whether it relates to a physical or mental health condition, the provision of healthcare, or the payment of healthcare. That's what constitutes PHI under HIPAA.”

A path forward would be to separate HIPAA identifiers from health information so that tools that don't sign BAAs never receive protected health information.



From there, this is a risk mitigation decision for healthcare organizations. Some will interpret that they need to do nothing, like on the right side of the graph below, and will continue leveraging all the advertising tools. The downside is that the native tracking pixels that power advertising tools are like signposts for lawyers and regulators to dig deeper. We've seen expensive and time-consuming class action lawsuits as the main risk of doing nothing.



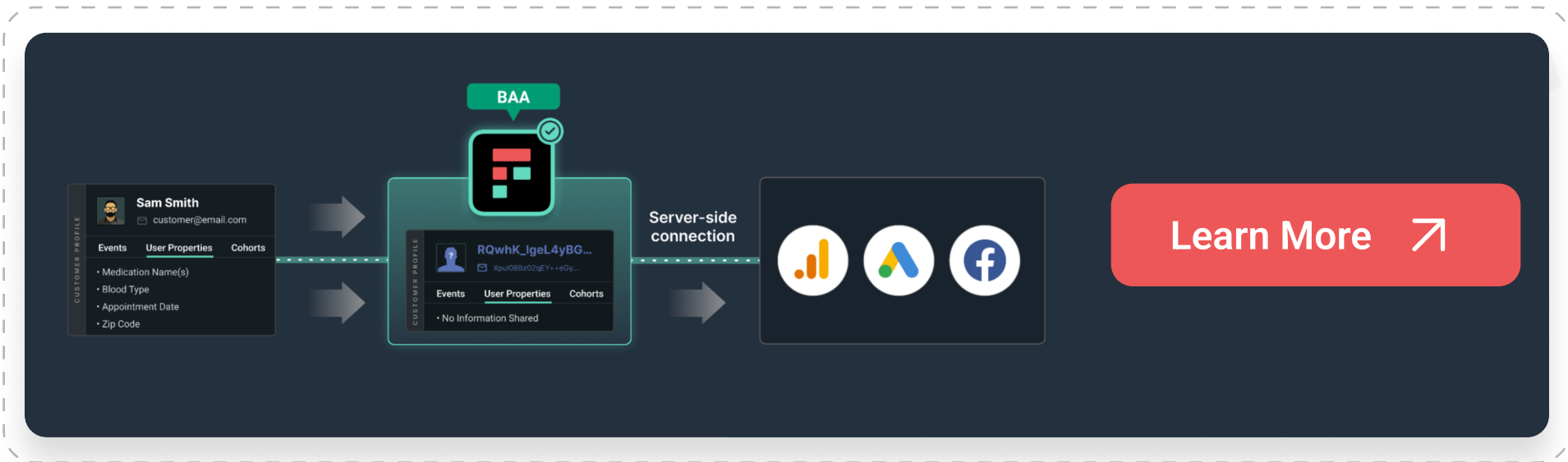
On the other end of the continuum, organizations could decide they need to abandon digital advertising channels altogether. If they're invested heavily in those areas, [the business impacts could be punishing](#).

The middle ground involves striving for high-performance results on digital channels with much more control over what data is shared with those tools.

This involves moving from third-party data, where native ad pixels sit on your site and collect what they want, to [a world of first-party data](#), where a [BAA-supported platform](#) replaces all the native trackers with one and gives the healthcare organization complete control over what data can be shared to advertising tools.

The Office for Civil Rights called out a solution in [their March 18, 2024, guidance](#) that involves replacing web tracking technologies that won't sign business associate agreements with tools like [Freshpaint](#) that sign BAAs and help govern the flow of data so PHI is never shared with downstream tools.

“If the chosen tracking technology vendor will not provide written satisfactory assurances in the form of a BAA that it will appropriately safeguard PHI, then the regulated entity can choose to establish a BAA with another vendor, for example a Customer Data Platform³⁹ vendor, that will enter into a BAA with the regulated entity to de-identify online tracking information that includes PHI and then subsequently disclose only de-identified information to tracking technology vendors that are unwilling to enter into a BAA with a regulated entity.



Replacing web trackers that won't sign BAAs with a tool like Freshpaint offers a HIPAA-compliant way of governing data flow to downstream tools.

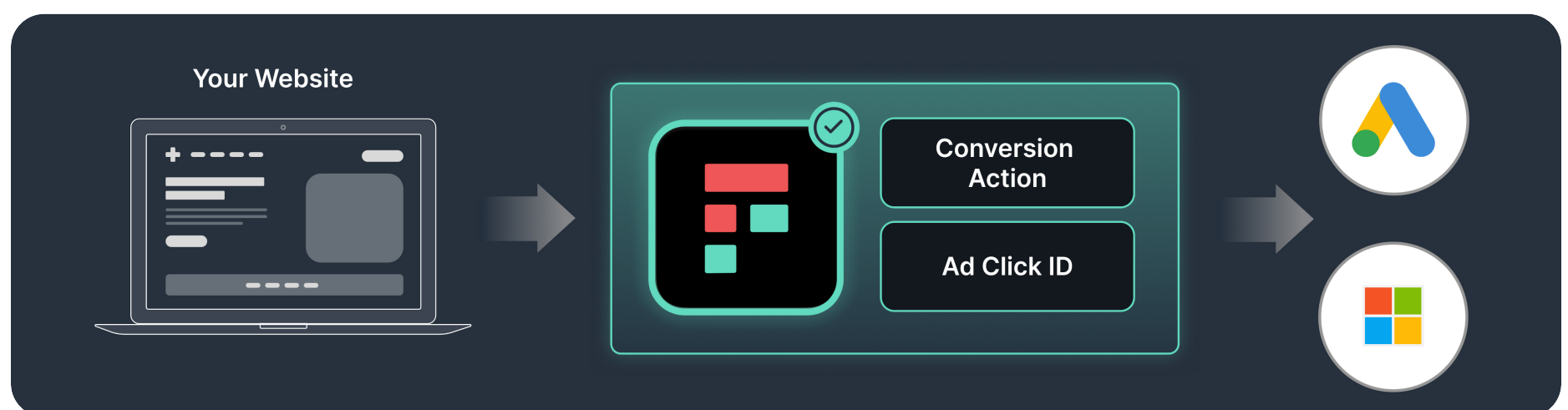
Advertising tools can be incredibly effective without receiving protected health information. Let's get into that.

Search Engine Advertising

Minimum Data Set Required

Search engine advertising native tracking pixels have access to identifiers like IP address and page visits by consumers visiting your site, inevitably sharing protected health information where BAAs do not exist.

But they don't need all of that data to perform. In testing with healthcare organizations, KPIs, like cost per lead and customer acquisition cost, stay stable when the data sharing is limited to those below:



Why This Doesn't Disclose PHI

The ad click ID contains a HIPAA identifier (created in a platform not covered by HIPAA, so no new information is being shared with the ad platform). The generic conversion action contains no information. It's just a "Yes, success happened."

Health information is missing from this equation. By limiting the data feedback to only the ad click ID and the generic conversion, a healthcare marketing team can continue to make a platform like Google Ads work without sharing PHI.

We asked Dori from Faegre Drinker to weigh in.

“*If an Ad Click ID is not connected to any healthcare information or the payment of healthcare services it would not constitute PHI. So you have to have that combination, the identification, and then does it relate back to the provision of healthcare services or the payment of healthcare services?*”

OCR was very specific in [the March 18, 2024, guidance](#) about the sharing of identifiers alone with a tracking technology on unauthenticated pages not being PHI:

“*For example, where a user merely visits a hospital’s webpage that provides information about the hospital’s job postings or visiting hours, the collection and transmission of information showing such a visit to the webpage, along with the user’s IP address, geographic location, or other identifying information showing their visit to that webpage, would not involve a disclosure of an individual’s PHI to tracking technology vendor. This is true even if there is a reasonable basis to believe that the information can be used to identify the user who visited the webpage, because the online tracking technologies in this example did not have access to information about an individual’s past, present, or future health, health care, or payment for health care.*”

Potential Objections

- When bidding on "diabetes type 2 treatment" and serving ads for it in Google Ads, isn't that a violation of HIPAA?
 - All keyword bidding and ad creatives live in the search engine advertising platform, which is not a covered entity and is not subject to HIPAA. Consumers who use search engines are subject to the terms and conditions of those platforms. Healthcare organizations need to pay careful attention to what data they share back to the ad platform after a user has clicked from an ad and visited their site.

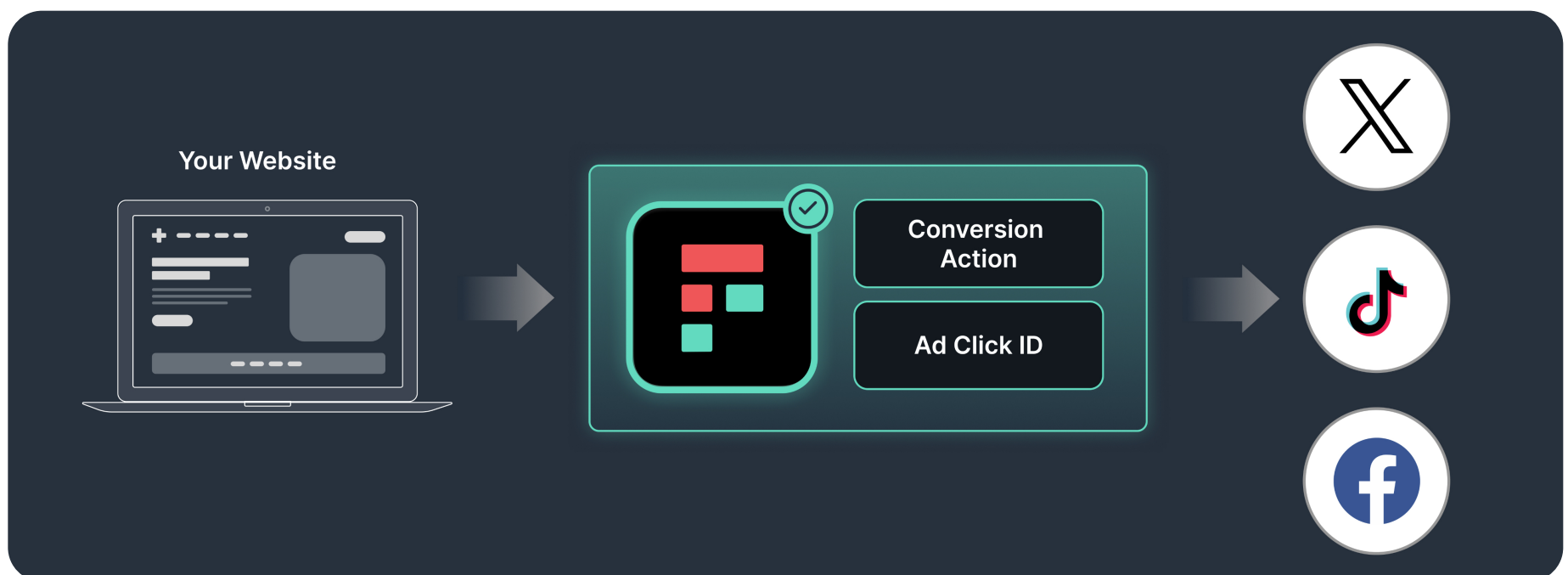
- The ad click ID is a HIPAA identifier. Wouldn't sharing that back to ad platforms be a violation of HIPAA?
 - While the ad click ID is a HIPAA identifier, sharing it alone is not protected health information. Additional health context, like the pages visited, would have to be included in the data sharing for it to be considered PHI. Additionally, the ad click ID originates in the ad platform and is not covered by HIPAA. Some legal teams interpret that sharing the ad click ID back to the ad platform does not introduce any new information that the ad platform didn't already have.

Direct Response Advertising

Minimum Data Set Required

Direct response advertising native tracking pixels collect information about consumers visiting a healthcare website site, inevitably sharing protected health information where BAAs do not exist.

However, just like search engine advertising platforms, they only need some of that data. In testing with healthcare organizations, KPIs like cost per lead and customer acquisition cost stay stable when just sharing the data points pictured below.





Why This Doesn't Disclose PHI

A HIPAA identifier is present in the ad click ID (created in the platform not covered by HIPAA, so no new information is being shared with the ad platform). The generic conversion action contains no information. It's just a "Yes, success happened."

Health information is missing from this equation. By limiting the data feedback to only the ad click ID and the generic conversion, a healthcare marketing team can continue to make a platform like Google Ads work without sharing PHI.

A reminder about the [March 18, 2024 Office for Civil Rights guidance](#) about tracking technologies on unauthenticated pages:

“For example, where a user merely visits a hospital’s webpage that provides information about the hospital’s job postings or visiting hours, the collection and transmission of information showing such a visit to the webpage, along with the user’s IP address, geographic location, or other identifying information showing their visit to that webpage, would not involve a disclosure of an individual’s PHI to tracking technology vendor. This is true even if there is a reasonable basis to believe that the information can be used to identify the user who visited the webpage, because the online tracking technologies in this example did not have access to information about an individual’s past, present, or future health, health care, or payment for health care.”

Potential Objections

- Wouldn't creating ads and serving them on a platform like Facebook violate HIPAA?
 - All audience building and ad creatives are built in the ad platform, which is not a covered entity and is not subject to HIPAA. Consumers who use social media platforms like Facebook are subject to the terms and conditions of those platforms. Healthcare organizations need to pay careful attention to what data they share back to the ad platform after a user has clicked from an ad and visited their site.
- The ad click ID is a HIPAA identifier. Wouldn't sharing that back to ad platforms be a violation of HIPAA?
 - While the ad click ID is a HIPAA identifier, sharing it alone is not protected health information. Additional health context, like the pages visited, would have to be included in the data sharing for it to be considered PHI. Additionally, the ad click ID originates in the ad platform and is not covered by HIPAA. Some legal teams interpret that sharing the ad click ID back to the ad platform does not introduce any new information that the ad platform didn't already have.

Programmatic Advertising

Minimum Data Set Required

Programmatic advertising relies on native tracking pixels intercepting activity and dropping third-party cookies into consumers' browsers visiting healthcare websites. Those pixels and cookies can capture and share PHI with third parties where a BAA doesn't exist.

The solution is to replace those native pixels and third-party cookies with [a tracking platform that signs a BAA](#) and then restricts the data flow to only a few key components.

You'll still need to share the ad click ID and the generic conversion action for clickthrough attribution. However, programmatic advertising relies heavily on view-through conversions since most users don't click display ads. They view them and convert on a later visit. For view-through conversions to work, the healthcare organization must share the IP address with the ad platform.



Why This Doesn't Disclose PHI

While the ad click ID and IP address are HIPAA identifiers, health information is missing from this equation. By limiting the data feedback to only the ad click ID, IP address, and generic conversion, a healthcare marketing team can continue to make programmatic ad platforms work without sharing PHI.

Here's what Dori Cain from Faegre Drinker states that you need to have the identifiers associated with health information for it to be PHI.

“*If you're not connecting the Ad Click ID and IP Address to the provision or payment of health care, then it does not constitute PHI under HIPAA.*”

OCR called out in [the March 18, 2024 guidance](#) that a HIPAA identifier like IP address in the absence of health information shared from an unauthenticated page is not PHI.



Potential Objections

- Sharing IP addresses violates HIPAA
 - In the HIPAA guidance, HHS was very clear that IP addresses on unauthenticated pages (like a public-facing website) need both the IP and health context for them to be considered PHI.
- Third-party cookies violate patient privacy
 - Third-party native pixels and cookies do put healthcare organizations at high risk of violating privacy laws. That's why a critical step is removing all those trackers and switching to a platform that uses a first-party tracker and cookie backed by a BAA-supported platform.

Retargeting

Minimum Data Set Required

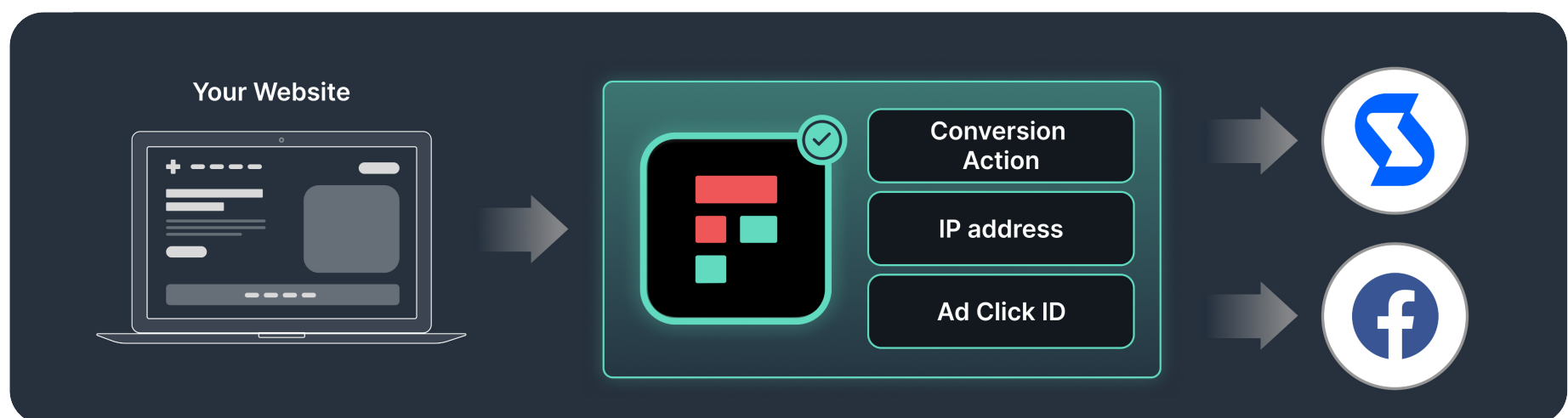
Retargeting relies on native tracking pixels intercepting activity and dropping third-party cookies into consumers' browsers visiting healthcare websites. Those pixels and cookies can capture and share PHI with third parties where a BAA doesn't exist.

The goal of retargeting is to re-engage consumers based on their previous visits to a healthcare website. It's a second chance to either move them further down the funnel we pictured at the beginning of this guide or to get that desirable final conversion.

How could this technically be done in a way that doesn't share PHI with those advertising tools?

Part one of the solution is to replace the native advertising web trackers and third-party cookies with a tracking platform that signs a BAA and then restricts the data flow to only a few key components.

In order to measure view-through and click-through conversions, the IP address and ad click IDs, along with a generic conversion action, need to be shared.



The second consideration is how the audience is being shared with the ad platform. Since the ad platform will receive HIPAA identifiers, it can never receive health information, or you'll risk a HIPAA violation. Platforms like [Freshpaint](#) can share those identifiers but block the sharing of any of the context or behavior during their visit, ensuring that no health context or information will be shared.

Finally, you have to consider the creative. If your creative is very narrow and specific to a condition or treatment, does that introduce health context in the creative itself? Does that feel "creepy"? Healthcare marketers may need to test more brand-oriented creative with "learn more" calls to action vs. treatment-specific creative with "schedule an appointment" calls to action.

Why This Doesn't Disclose PHI

While the ad click ID and IP address are HIPAA identifiers, health information is missing from this equation. By limiting the data feedback to only the ad click ID, IP address, and generic conversion, a healthcare marketing team can continue to make retargeting platforms work without sharing PHI.

Once again, you'll need to carefully consider the creative since the audience is being introduced from behaviors on the healthcare website. Brands that find ways to leverage retargeting in healthcare are likely going to test ways to use higher funnel brand creative vs. treatment or condition-specific creative.

Potential Objections

- Sharing IP addresses violates HIPAA
 - In the HIPAA guidance, HHS was very clear that IP addresses on unauthenticated pages (like a public-facing website) need both the IP and health context for them to be considered PHI.
- Third-party cookies violate patient privacy
 - Third-party native pixels and cookies do put healthcare organizations at high risk of violating privacy laws. That's why a critical step is removing all those trackers and switching to a platform that uses a first-party tracker and cookie backed by a BAA-supported platform.
- Since the healthcare marketer is introducing the audience based on website behavior that is going to introduce PHI
 - Tools like Freshpaint can introduce an audience but block all context about their journey through the website from being shared with the advertiser. HIPAA identifiers will be shared, but no health information is provided to the ad platform.

- Introducing ad creative that is condition or treatment-specific, or introduces a narrow call to action could be introducing health information to the ad platform.
 - We actually agree with this objection. Healthcare marketing and legal teams will have to carefully discuss which types of ad creative would be acceptable to introduce to ad platforms in a retargeting scenario.

Make Digital Ad Platforms High Performance & HIPAA-Compliant

[Learn more ↗](#)

Your Website

Facebook, Google Analytics, Microsoft

Conclusion

Digital advertising is a powerful way for healthcare marketers to reach today's consumers where they are. But continuing to utilize advertising tools in exactly the same way we have for the last decade puts our healthcare organizations at risk. What to do?

On one hand moving off these channels reduces our ability to connect with future patients and improve their health outcomes. On the other hand, continuing to freely share data to advertising tools that won't sign business associate agreements puts patient privacy at risk and opens up healthcare organizations to lawsuits, fines, and an erosion of brand trust.

Moving forward means continuing to use the full power of the Internet but in a privacy first way. In order to do that we need to continue to monitor how these tools work and find ways to govern the flow of information to them in a way that makes them work for us without every sharing our visitor or patient sensitive information.

About Freshpaint

Freshpaint is a Healthcare Privacy Platform that bridges the gap between patient privacy and digital marketing by ensuring sensitive data is never shared with tools that aren't HIPAA-compliant. Freshpaint replaces untrusted tracking technologies from tools like Google Analytics, Facebook, and Google Ads, then provides a governance layer that controls what data gets shared with those platforms.

Want to keep learning?

Visit [Freshpaint.io](https://freshpaint.io) ↗

Contact us at sales@freshpaint.io ↗

Connect with us on [LinkedIn](#) ↗

Meet with us ↗

