



# HIPAA, FTC, & State Laws – What you need to know NOW!

Jenny Bristow, CEO, Hedy & Hopp





# Jenny Bristow, CEO of Hedy & Hopp

Hedy & Hopp is passionate about improving patients' access to care through smarter patient–direct and physician marketing programs.

***All of H&H's work is based in the foundation of creating joy and positivity - because the work we do changes lives, and it should be fun!***

Prior to starting H&H, Jenny launched, grew and sold a digital agency in Seattle and worked at Amazon.

H&H was named Fastest Growing Company in St. Louis by *Small Business Monthly* in 2018 and 2019 and the #1 Fastest Growing Company in St. Louis by the *St. Louis Business Journal* in 2019. Jenny was named a St. Louis Titan (one of the 100 most influential people in St. Louis) in 2021 and a top female business owner in 2023.

She loves teaching others about the more technical aspects of healthcare marketing, making it easy to understand and fun!





## Quick Disclaimer:

This is not intended to be legal direction or guidance, but a tool to reference the high-level details of these laws that impact marketing activities.

# What will we cover today?

The legal landscape is constantly shifting in healthcare marketing, and the rules tightened even more in 2022.

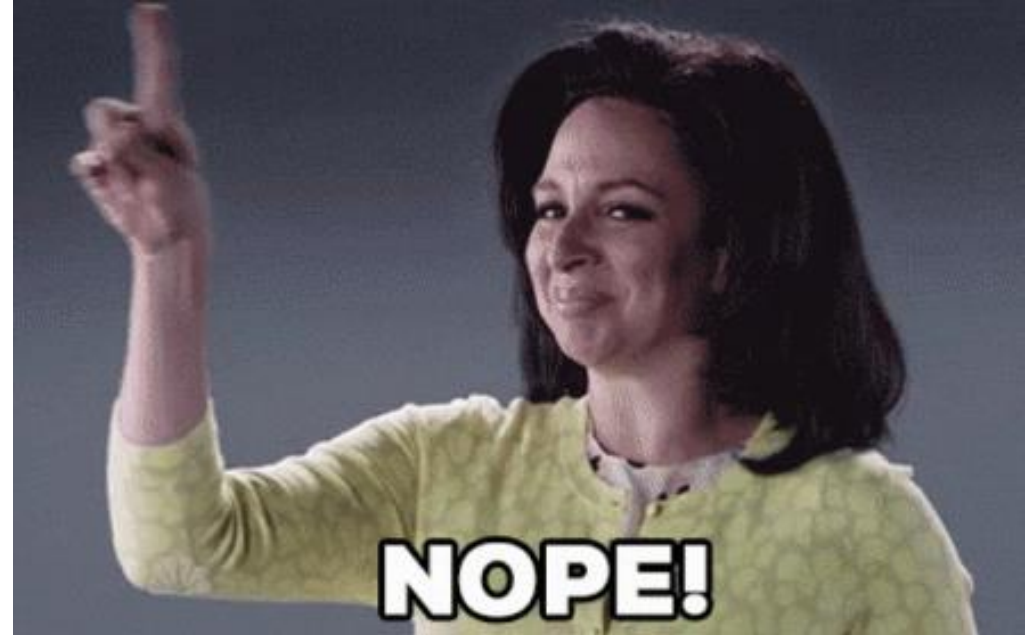
Let's talk about what can you track, what can't you track, and **why!**

## Today's Learning Objectives:

- Understand what changes happened in 2022 regarding digital marketing and patient privacy.
- Learn what questions you should be asking your internal and agency teams to ensure compliance.
- Understand best practices to track the patient journey online – what you can and can't do.

# What are we not going to do today?

Pitch a proprietary tool that my company has developed.

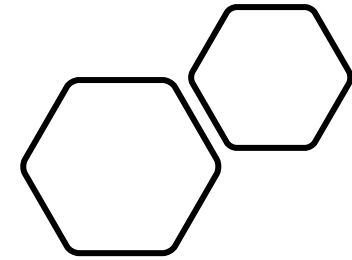


**Who attended a session  
last year about patient  
marketing attribution?  
Determining ROI?  
Creating a dashboard?**





**EVERYBODY PANIC!**



# What are we going to focus on today?



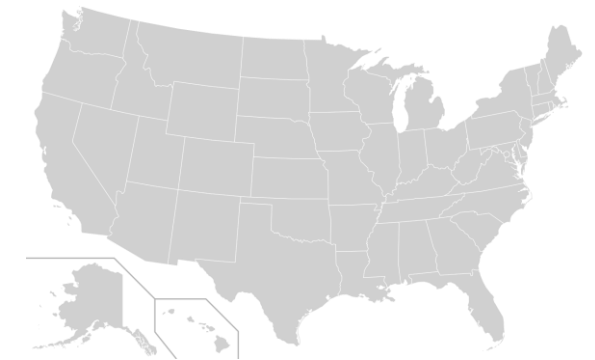
**HIPAA  
(OCR & HHS)**



**FTC**



**GDPR  
(Just a bit)**



**State  
Privacy Laws**



# HIPAA – What Changed?

- A new bulletin was released by OCR/HHS in December 2022.
  - Bulletin = Guidance, NOT new law.
- It clarified that **IP addresses for users on a marketing website ARE PHI.**
  - And even if you tell a tool to NOT collect it, if it CAN collect it – you're in violation.
- It also reinforced importance of having a BAA with any tech vendor that can see IP address (or device ID, etc.)
- And, it specifically calls out service-line or symptom-specific pages as a concern.

**This means if you use a typical Google Analytics setup (GTM and GA), you are in violation. (And, no, GA4 doesn't fix this.)**

## References:

[Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates – Bulletin December 2022](#)

# HIPAA – What did these changes sound like?

*“All such IIHI collected on a regulated entity’s website or mobile app generally is PHI, **even if the individual does not have an existing relationship with the regulated entity** and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”*

*“...thus relates to the individual’s **past, present, or future** health or health care or payment for care.”*

## References:

[Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates – Bulletin December 2022](#)

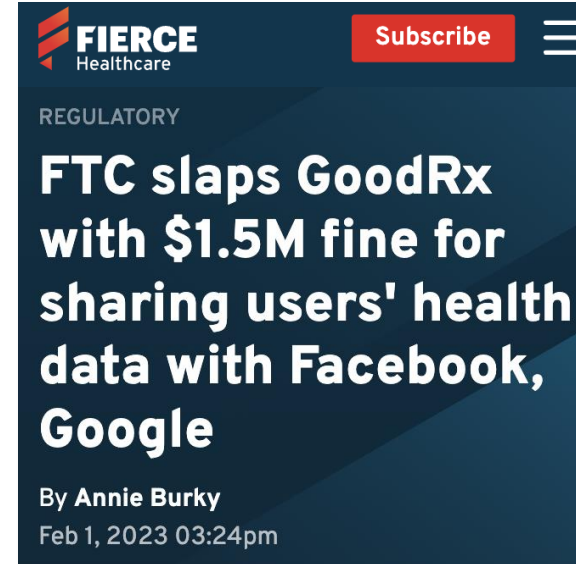
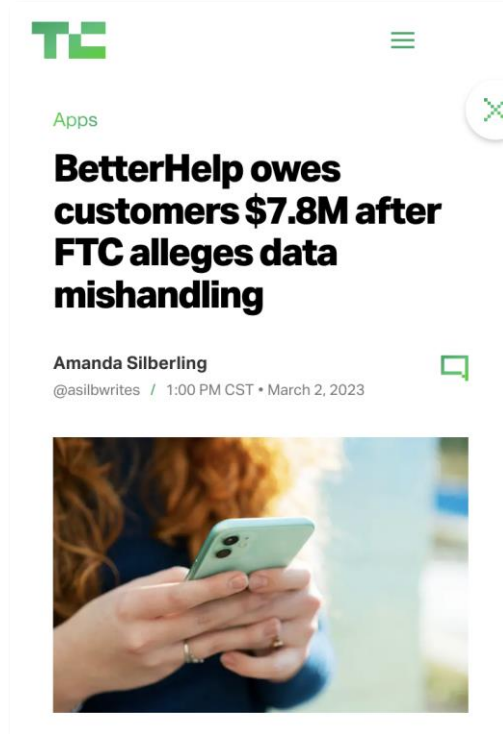
# FTC – What Changed?

- Angry that healthcare adjacent companies (non-covered entities) are selling data to third parties without consent.
- Really, selling data?
- **YES** – Meta’s pixel shares information back to advertisers about conversions. This is legally ”consideration” = selling data.
- The FTC also believes consumers don’t know enough/wouldn’t agree, even if privacy policies included language disclosing the transaction.
  - So, just disclosing what you’re doing as a solution doesn’t work.

## References:

[BetterHelp](#) and [GoodRx](#) settlement details; [Blog post “guidance” from FTC](#), March 2023

# FTC – Impact of This Position



**Both fines came as a result of using Meta pixels to track conversions!**

# And then, the HHS & FTC joined forces.



## References:

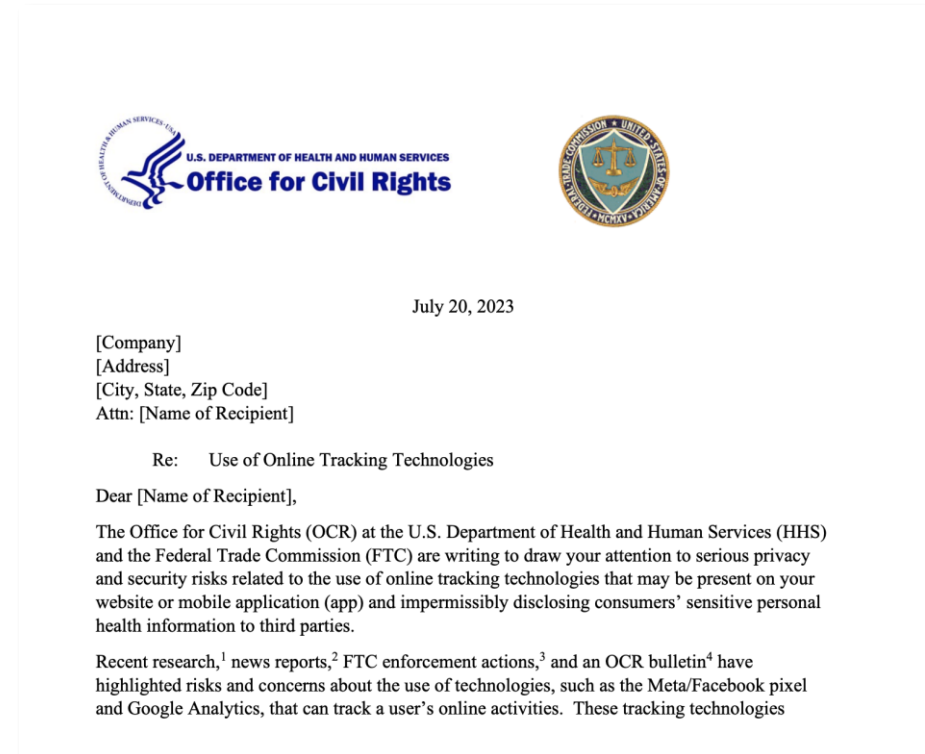
[FTC and HHS issue joint letter to 130 telehealth providers and hospitals](#), July 2023

[Model Letter: Use of Tracking Technologies](#)

# 130 hospital systems and telehealth providers – you’ve got mail!



The screenshot shows the top of a press release page from the Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services (HHS). The page includes the FTC logo and navigation links for Enforcement, Policy, Advice and Guidance, News and Events, and About the FTC. The breadcrumb trail reads: Home / News and Events / News / Press Releases. A 'For Release' button is visible. The main title is 'FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies'. Below the title is a sub-headline: 'Letters highlight concerns stemming from use of technologies that may share a user's sensitive health information'. The date is July 20, 2023, with social media icons for Facebook, Twitter, and LinkedIn. Tags include Consumer Protection, Bureau of Consumer Protection, Health, Privacy and Security, Consumer Privacy, and Health Privacy. Related resources include a model letter titled 'Use of Online Tracking Technologies'. The bottom of the page begins with 'The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.'



The image shows the content of a joint letter from the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC). The letter is dated July 20, 2023. The recipient information is redacted with placeholders: [Company], [Address], [City, State, Zip Code], and Attn: [Name of Recipient]. The subject line is 'Re: Use of Online Tracking Technologies'. The salutation is 'Dear [Name of Recipient],'. The main body of the letter states: 'The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties. Recent research,<sup>1</sup> news reports,<sup>2</sup> FTC enforcement actions,<sup>3</sup> and an OCR bulletin<sup>4</sup> have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

## References:

[FTC and HHS issue joint letter to 130 telehealth providers and hospitals, July 2023](#)

[Model Letter: Use of Tracking Technologies](#)

# GDPR

In the U.S., do you need to comply with GDPR?

The biggest points to consider:

**Opt-In vs.  
Opt-Out**

**Right to Be  
Forgotten**

# But, don't forget about state laws!

## CALIFORNIA – JANUARY 1, 2023

- ✓ allow consumers to opt-out of the sales of personal info
- ✓ honor opt-out preference signals or GPCs
- ✓ allow consumers to limit the processing of sensitive personal info
- ✓ implement data minimization and purposes limitation principles
- ✓ honor CPRA consumer requests
- ✓ provide a privacy notice
- ✓ ensure service providers comply with the law
- ✓ establish a data retention period

!! will likely soon require data brokers to disclose what they collect and allow consumers to direct brokers to delete their personal info

## CONNECTICUT – JULY 1, 2023

- ✓ allow consumers to opt-out of the processing of sensitive personal info
- ✓ collect and process only the minimum amount of data needed for the processing purpose
- ✓ provide a privacy notice
- ✓ conduct data protection impact assessment where there is a risk

!! will likely soon require to honor opt-out preference signals or GPCs

## VIRGINIA – JANUARY 1, 2023

- ✓ allow consumers to opt-out of the sales of personal info, targeted advertising, and profiling
- ✓ ensure data processing agreements are in place with data processors
- ✓ provide a privacy notice
- ✓ honor consumer requests
- ✓ conduct privacy impact assessment if required for your processing activities

## COLORADO – JULY 1, 2023

- ✓ provide consumers to opt-out of the sales of personal info, targeted advertising, and profiling
- ✓ provide a privacy notice
- ✓ conduct data protection impact assessment where there is a risk
- ✓ honor consumer requests

!! will likely soon require to honor opt-out preference signals or GPCs



# And, more are on the way!

## UTAH – DECEMBER 31, 2023

- ✓ honor consumer requests
- ✓ allow consumers to opt-out of the sales of personal info or from targeted advertising
- ✓ have processing agreements in place
- ✓ provide a privacy notice

## IOWA – JANUARY 1, 2025

- ✓ limit data processing to the specified purposes
- ✓ provide a privacy notice
- ✓ allow consumers to opt-out of the sales of personal info
- ✓ have written contracts with service providers
- ✓ honor consumer requests for access, deletion, portability, opt-out, etc.

## INDIANA – JANUARY 1, 2026

- ✓ allow consumers to opt-out of the sales of personal info
- ✓ obtain explicit consent for the processing of sensitive personal data
- ✓ limit processing to intended purposes
- ✓ honor consumer requests
- ✓ provide a comprehensive privacy notice
- ✓ conduct data impact assessment in the case of targeted advertising

## MONTANA – OCTOBER 1, 2024

- ✓ respond to consumer requests
- ✓ allow consumers to opt-out of the sales of personal info
- ✓ recognize universal opt-out mechanisms
- ✓ provide a privacy notice and a privacy policy
- ✓ obtain explicit consent before collecting sensitive data
- ✓ conduct data protection impact assessments for processing sensitive data, selling data, or using data for targeted advertising and/or profiling

!! will likely soon require to honor opt-out preference signals or GPCs

## TENNESSEE – JULY 1, 2025

- ✓ honor consumer requests to know, access, delete, etc.
- ✓ allow consumers to opt-out of the sales of their data
- ✓ have written contracts with service providers
- ✓ provide a privacy notice and a privacy policy
- ✓ process the data only for the purposes it has been collected for

This is not intended to be legal direction or guidance, but a tool to reference the high-level details of these laws that impact marketing activities.

# Okay, so which entities do YOU need to consider?

**Hedy & Hopp's POV is that both covered and non-covered entities need to understand and address all regulations and case law regarding patient privacy.**



# Key questions you need to answer...

1. What tools are we currently using in our digital ecosystem?
2. What patient/user information are we capturing, where is it being stored, and who has access to it?
3. What are the key things we're doing that are of immediate concern related to patient privacy?
4. How can we continue doing the marketing tactics we need to be successful, but in a compliant way?

**...and a process to get there.**



# Step 1: Audit It All

Organizing tools into categories helps team members and agency partners think comprehensively

How big of a risk is this tool?

PRIORITY LEVEL	ADVERTISING/MARKETING	ANALYTICS	WEBSITE EXPERIENCE	DEVELOPMENT & TECHNOLOGY
PRIORITY 1	<ul style="list-style-type: none"> <li>• Google Ads (AdWords)</li> <li>• Google Marketing Platform (GMP)</li> <li>• LinkedIn Insight Tag</li> <li>• Meta/Facebook</li> <li>• Microsoft Advertising (with Microsoft Clarity)</li> </ul>	<ul style="list-style-type: none"> <li>• Google Analytics</li> <li>• Google Tag Manager</li> <li>• Looker*</li> </ul>	<ul style="list-style-type: none"> <li>• Wistia</li> </ul>	
PRIORITY 2	<ul style="list-style-type: none"> <li>• Accretive Media</li> <li>• Social Share buttons</li> </ul>		<ul style="list-style-type: none"> <li>• Crazy Egg</li> <li>• Optimizely</li> <li>• Osano</li> </ul>	<ul style="list-style-type: none"> <li>• Anti-Spam Reloaded</li> <li>• Cloudflare</li> <li>• iThemes Security</li> <li>• miniOrange SSO using SAML 2.0</li> <li>• MySQL</li> <li>• Wordpress Engine</li> </ul>

Most audits uncover 50-75 tools across these four categories.

Pro tip – use [www.builtwith.com](http://www.builtwith.com) to find tags!

# Step 2: Understand Where Patient Data Is Collected & Shared

SOFTWARE/TACTIC	CATEGORY	DESCRIPTION	DATA READ, COLLECTED, OR/AND SHARED <small>(if applicable)</small>
Google Analytics	Analytics	<p>Google Analytics is a web analytics service offered by Google that allows website owners to track and analyze website traffic, user behavior, and other important metrics. It provides detailed insights into how users interact with a website, including information on where they come from, what pages they visit, how long they stay, and what actions they take. This information can be used to optimize website performance, improve user experience, and create more effective marketing campaigns.</p>	<p>Google Analytics stores a client ID in a first-party cookie named "_ga" to distinguish unique users and their sessions on your website. By default it collects the following information:</p> <ul style="list-style-type: none"> <li>• User and Session data - Includes the volume of each as well as rate metrics</li> <li>• HTTP Headers – Includes IP addresses and information about the web browser, like page location, document, referrer, and the person using the website</li> <li>• Geolocation using IP Address - Google Analytics 4 masks the last digits and doesn't store or log the IP addresses</li> <li>• Device Information - This includes the device and operating system information</li> <li>• Page Information - Includes page URL, click URL, hostname, page title, etc.</li> </ul>
Google Marketing Platform (GMP)	Advertising/Marketing	<p>Floodlight is the conversion tracking system for Google Marketing Platform (Search Ads 360, Display &amp; Video 360, and Campaign Manager 360) used to track and report conversions, using a measurement pixel that is installed on the webpage. When a customer lands on the conversion page, the tag sends data about the conversion to the GMP product, that can be used in other tactics, such as retargeting.</p>	<p>PHI/PII is collected through the following ways:</p> <ul style="list-style-type: none"> <li>• When advertisers manually send PHI/PII data when using enhanced conversions</li> <li>• When PII/PHI gets manually sent through the "Floodlight Variables" for audience remarketing</li> <li>• When floodlight activity is tracking an action that violates HIPAA policy, for example account sign, visits to specific health condition page, etc.</li> </ul>

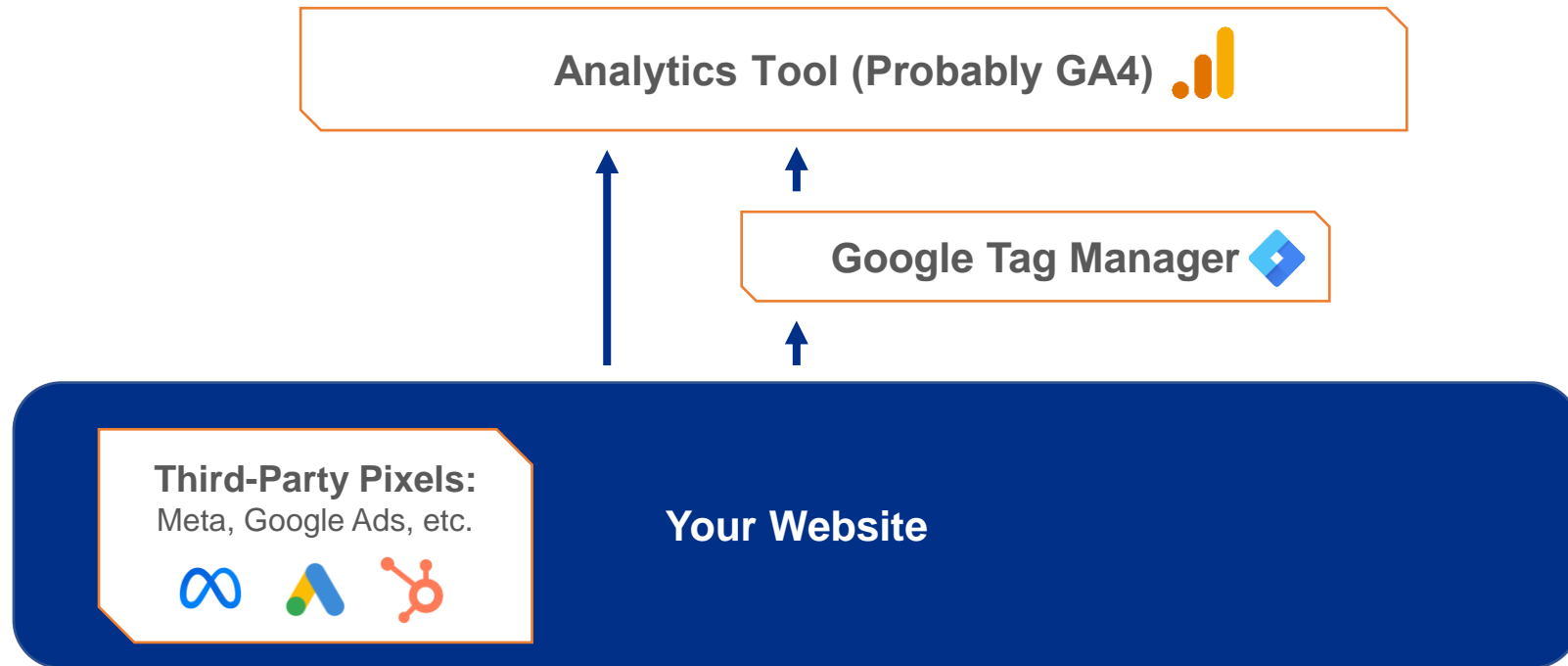
# Step 3: Clean-Up for the Short Term

- Remove non-compliant tools **ASAP**
  - Google Analytics
  - Any third-party trackers/pixels (Meta, LinkedIn, Google Ads, etc.)
- Yes, there will be a gap in tracking. It's worth it!
- Notify your legal & compliance team of tools removed
- Develop your strategy to rebuild your marketing analytics in a compliant way – see Step 4!



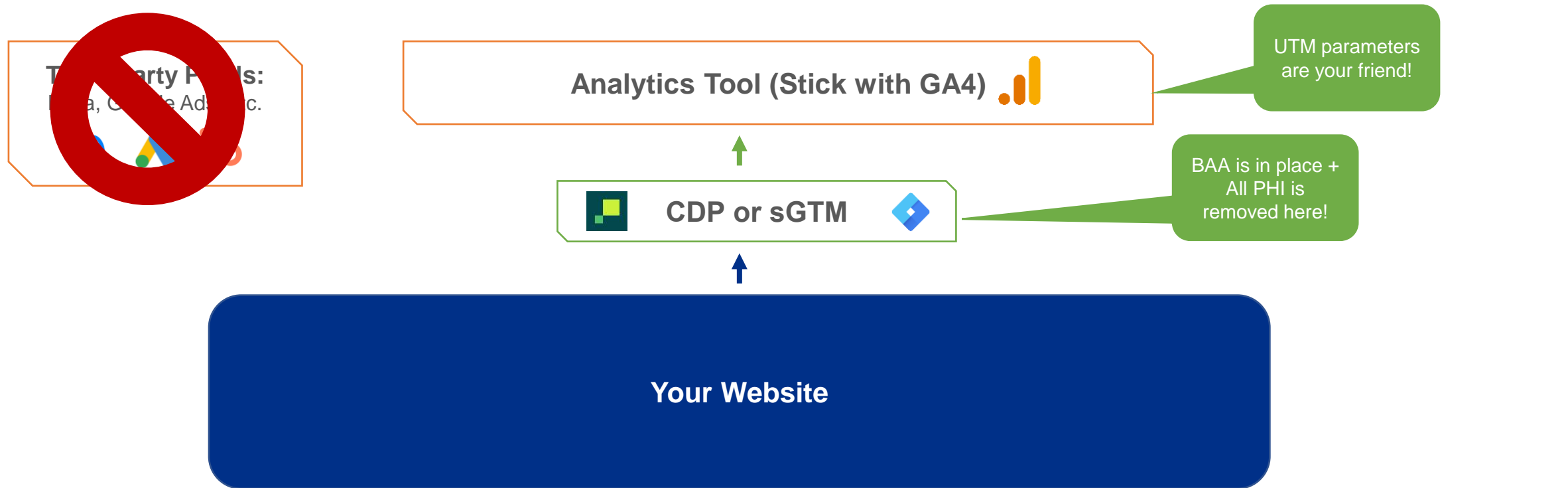
# Step 4: Rebuild Analytics Infrastructure for the Long-Term

Today's Typical Marketing Analytics Structure:



# Step 4: Rebuild Analytics Infrastructure for the Long-Term

## Marketing Analytics Structure for Healthcare – Option 1:



CDP = Customer Data Platform  
sGTM = server-side Google Tag Manager

# Step 4: Rebuild Analytics Infrastructure for the Long-Term

## Marketing Analytics Structure for Healthcare – Option 2:



New Analytics Tool (Piwik Pro, Mixpanel, Adobe)

UTM parameters are (still) your friend!

BAA is in place!

Your Website

# Let's weigh the options:

		Option 1	Option 2
		Server-Side Google Tag Manager (sGTM)	Customer Data Platform (CDP)
<b>Pros</b>		<ul style="list-style-type: none"> <li>Less cost</li> <li>Keep using familiar tools</li> </ul>	<ul style="list-style-type: none"> <li>Will sign a BAA</li> </ul>
<b>Cons</b>		<ul style="list-style-type: none"> <li>Internal team (or agency partner) needs deep analytics knowledge</li> <li>Time/Cost to implement</li> </ul>	<ul style="list-style-type: none"> <li>Will sign a BAA</li> <li>Cost to buy tool (and ongoing cost)</li> <li>Time/Cost to implement</li> </ul>
<b>Tool Options</b>		Stay with Google Analytics / GTM!	<ul style="list-style-type: none"> <li>Hightouch</li> <li>FreshPaint</li> <li>Segment</li> </ul>

**Following these steps will help you continue doing the marketing tactics you need to be successful – but in a compliant way.**



# What to do when you get home?

Knowledge (and cross-functional alignment) are power!

Start with asking questions to your internal teams and agency partners – find our list in your conference app!

## SHSMD 2023

### HIPAA, FTC & STATE LAWS – WHAT YOU NEED TO KNOW NOW!

#### WHAT'S NEXT?

#### KEY QUESTIONS TO ASK YOUR IN-HOUSE & AGENCY TEAMS

You've learned how guidelines around patient privacy and data collection have changed in the past year and what you can and cannot do when it comes to tracking the patient journey online. But, as a healthcare marketer, where do you go from here to make sure YOUR specific practices are really compliant?

Start by talking to your cross-functional teams – including Legal, IT, and any marketing agencies you work with. Use these questions to help determine your next steps and get back to what you really love – marketing.

#### HERE'S WHAT TO ASK YOUR...

##### ...MARKETING AGENCY

- How have you adjusted your practices and recommendations for healthcare clients based on the 12/2022 HHS bulletin?
- Please provide a list of any third-party tools or technologies that are being used on our website (think website hosting, video players, UX/heatmapping tools, etc.).
- What third-party tags, trackers, or pixels have been placed on our website, and how?
- Are you currently building any remarketing and/or look-alike audiences on any ad platform for our business?

##### ...LEGAL / COMPLIANCE / PRIVACY TEAMS

- What is our organization's position on the 12/2022 HHS bulletin about HIPAA and recent FTC rulings?
- What state and/or industry-specific laws do our organization's marketing practices need to abide by (CCPA, GINA, etc.)?
- What marketing technology providers do we currently have contracts with? Have any signed BAAs?

##### ...IT / TECHNOLOGY TEAM

- What solutions in our patient-facing technology stack are collecting or exposed to PHI or PII (this INCLUDES IP address)?
- What is our organization's capability and comfort level implementing server-side analytics solutions (i.e., server-side Google Tag Manager)?

[www.HedyandHopp.com](http://www.HedyandHopp.com)



Health Care  
Strategy & Market  
Development™



# Questions?

Please be sure to complete the session evaluation!

