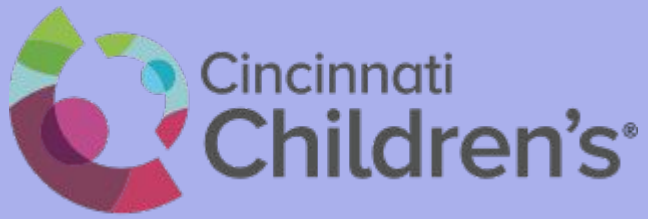


HIPAA, FTC, AND STATE LAWS: WHAT YOU NEED TO KNOW NOW

Aaron Williams, Cincinnati Children's Hospital
Jenny Bristow, Hedy & Hopp
HCIC 2023

AARON WILLIAMS, DIGITAL ANALYTICS & SEO MANAGER CINCINNATI CHILDREN'S

Cincinnati Children's is a nonprofit, comprehensive pediatric health system. As a leader in research and education, Cincinnati Children's is consistently ranked as one of America's best children's hospitals by *U.S. News & World Report* and is one of the top recipients of pediatric research grants from the National Institutes of Health.

Aaron joined Cincinnati Children's in 2011 as web editor supporting the research foundation. Since that time, Aaron has created the Digital Analytics & SEO Team at Cincinnati Children's and now leads a team of analysts dedicated to understanding and improving our users' digital experience.

Aaron lives in Cincinnati with his wife Kathy, and two boys Jack and Harrison. He is not a lawyer and probably gives terrible legal advice.

JENNY BRISTOW, CEO OF HEDY & HOPP

Hedy & Hopp is a full-service, fully healthcare agency that works with providers across the country.

Prior to starting H&H 8 years ago, 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!

Finally, she is a reluctant healthcare privacy expert.

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 2023.

Let's talk about which analytics tools and marketing tactics you can continue using, which you can't, and why!

Today's Learning Objectives:

- Understand what changes happened in 2022 (and 2023) 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 user journey online and what you can and can't do.

WHAT ARE WE NOT GOING TO DO TODAY?

Pitch a proprietary tool that we developed

WHO ATTENDED A SESSION LAST YEAR ABOUT MARKETING ATTRIBUTION? DETERMINING ROI? CREATING A DASHBOARD?


EVERYBODY PANIC!

WHAT ARE WE GOING TO FOCUS ON TODAY?

Dept. of Health and Human Services (HHS) Office for Civil Rights (OCR)

FTC

GDPR
(Just a bit)

State Privacy Laws

HIPAA – WHAT CHANGED?

A new bulletin was released by HHS/OCR in December 2022 (Bulletin = Guidance, NOT new law).

Two important points emerged:

1. It clarified that IP addresses for users on a marketing website ARE PHI.
   - Even if you tell a tool to NOT collect it, if it CAN collect it – you're in violation.

2. 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 it.)

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

HIPAA - WHAT DOES THIS MEAN FOR YOU?

DIGITAL HEALTHCARE MARKETING HAS TO MATURE

We won the “Digital Front Door” argument

IP|Unique Identifying ID + Health Information (Condition|Treatment|Service|Doctor|Scheduling) = PHI

PHI is PHI

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.

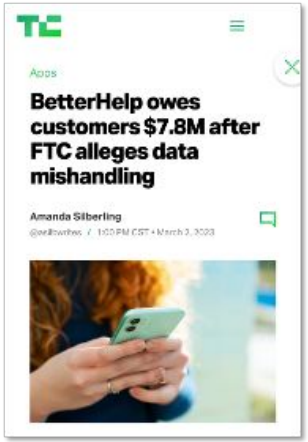
This is legally "consideration" = selling data.

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 META PIXELS TO TRACK CONVERSIONS

References:
BetterHelp and GoodRx settlement details; Blog post "guidance" from FTC, March 2023

AND THEN, HHS & THE FTC JOINED FORCES

130 HOSPITAL SYSTEMS AND TELEHEALTH PROVIDERS – YOU'VE GOT MAIL!

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement · Policy · Advice and Guidance · News and Events · About the FTC ·

Home / News and Events / News / Press Releases

For Release

FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies

Letters highlight concerns stemming from use of technologies that may share a user's sensitive health information

July 20, 2023

Tags: Consumer Protection | Bureau of Consumer Protection | Health | Privacy and Security | Consumer Privacy | Health Privacy

The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for

Related resources

Model Letter: Use of Online Tracking Technologies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

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,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] 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

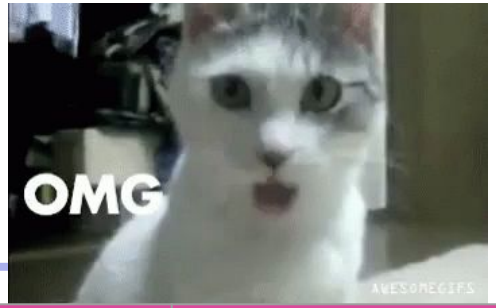
GDPR – IN THE U.S., DO YOU NEED TO COMPLY WITH GDPR?

THE BIGGEST POINTS TO CONSIDER

1. Opt-in vs. Opt-out
2. Right to be Forgotten

References:
Osano's Guide to GDPR

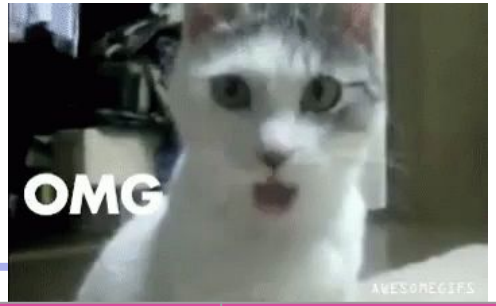
STATE LAWS – DON'T FORGET



CALIFORNIA JANUARY 1, 2023	CONNECTICUT JULY 1, 2023	VIRGINIA JANUARY 1, 2023	COLORADO JULY 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*	• 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*	• 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	• 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*

References:
BetterHelp and GoodRx settlement details; Blog post "guidance" from FTC, March 2023

STATE LAWS – MORE ARE ON THE WAY



UTAH DECEMBER 31, 2023	IOWA JANUARY 1, 2025	INDIANA JANUARY 1, 2026	MONTANA OCTOBER 1, 2024	TENNESSEE JULY 1, 2025
• 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	• 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.	• 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	• 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*	• 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

References:
BetterHelp and GoodRx settlement details; Blog post "guidance" from FTC, March 2023

OKAY, SO WHICH RULES DO YOU NEED TO CONSIDER?

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

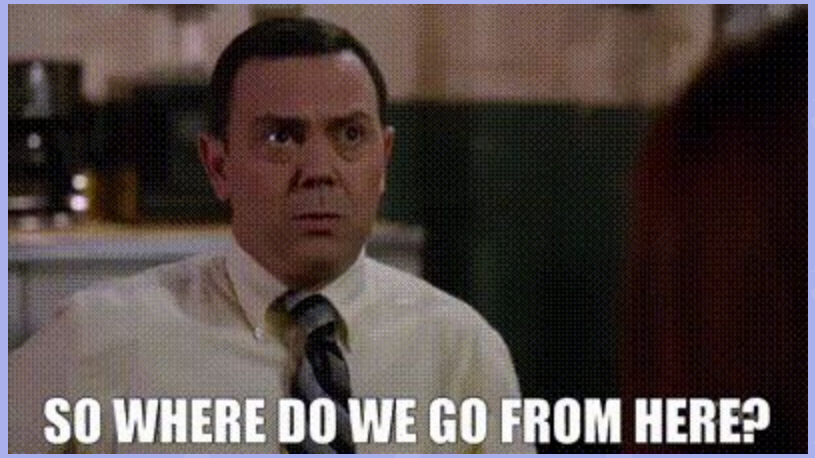
SAVE YOURSELF SOME TIME

Who is responsible for this work?

Probably no one/ not you

How do we get this work done?

You don't


SO WHERE DO WE GO FROM HERE?

GETTING STARTED

1. Identify Your Team
2. Build Understanding
3. Get Buy-in
4. Begin

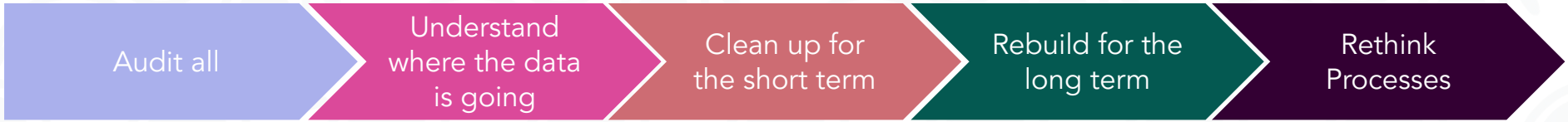
BUILDING YOUR TEAM

PARTNER	REASON TO CARE	PROBLEM TO SOLVE	DECISION TO MAKE
WEBSITE/ ANALYTICS	Would like to track and improve the performance of the website.	Current setup is "probably" not compliant.	Identifying the tools/technologies absolutely necessary for the web experience. Identifying the information collected and the compliance of the tool.
LEGAL/ COMPLIANCE	This is a system wide risk regarding the handling of PHI. This is not a question that can be answered by marketers alone.	Help apply the organization's broader legal understanding and risk tolerance to this evolving privacy challenge.	Does this decision fulfill our legal obligations and comply with the system's broader interpretation and procedures.
PAID MARKETING/ AGENCY PARTNERS	Wants to measure the effectiveness of marketing campaigns and improve the performance of campaigns in market.	Current set up is *definitely* not compliant. IP/URL/Conversion actions can not be shared with third parties that do not sign a BAA. Third parties will not sign a BAA.	Can campaigns be evaluated using first party data? If third party tools are necessary, why, and how can they be used in compliance with HHS/OCR?
IT/IS/SECURITY	Their support and expertise will be required regardless of the decisions made.	Evaluate and sign off on tools/technologies.	Which tools best fit into your current tech-stack and can be supported long-term.

KEY QUESTIONS 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?

THE PROCESS TO GET THERE



STEP 1: AUDIT 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	• Google Ads (AdWords) • Google Marketing Platform (GMP) • LinkedIn Insight Tag • Meta/Facebook • Microsoft Advertising (with Microsoft Clarity)	• Google Analytics • Google Tag Manager • Looker*	• Wistia	
Priority 2	• Accretive Media • Social Share buttons		• Crazy Egg • Optimizely • Osano	• Anti-Spam Reloaded • Cloudflare • iThemes Security • miniOrange SSO using SAML 2.0 • MySQL • Wordpress Engine

EXAMPLE ONLY!

Most audits cover 50-75 tools across these four categories

Pro tip: use 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 (IF APPLICABLE)
Google Analytics	Analytics	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.	Google Analytics stories client ID in a first-part cookie named "...ga" to distinguish unique users and their sessions on your website. By default, it collects the following information: • User and Session data: includes volume of each as well as rate metrics • HTTP Headers: includes IP addresses and information about the web browser, like page location, document, referrer, and the person using the website • Geolocation using IP address: Google Analytics 4 masks the last 4 digits and doesn't store or log the IP addresses • Device information: This includes the device and operating system information • Page Information: includes page URL, click URL, hostname, page title, etc.
Google Marketing Platform (GMP)	Advertising / Marketing	Floodlight is the conversion tracking system for Google Marketing Platform (Search Ads 360, Display & 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.	PHI/PII is collected through the following ways: • What advertisers manually send PHI/PII data when using enhanced conversions • When PHI/PII gets manually sent through the "Floodlight Variables" for audience remarketing • When floodlight activity is tracking an action that violates HIPAA policy, for example account sign, visits to specific health condition pages, etc.

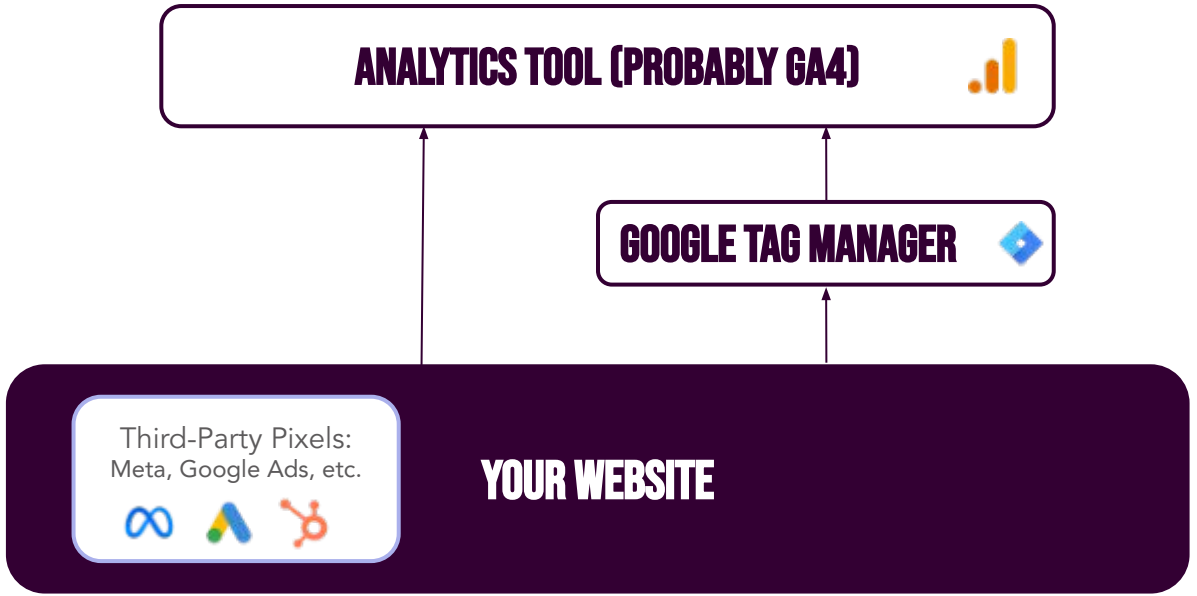
EXAMPLE ONLY!

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!

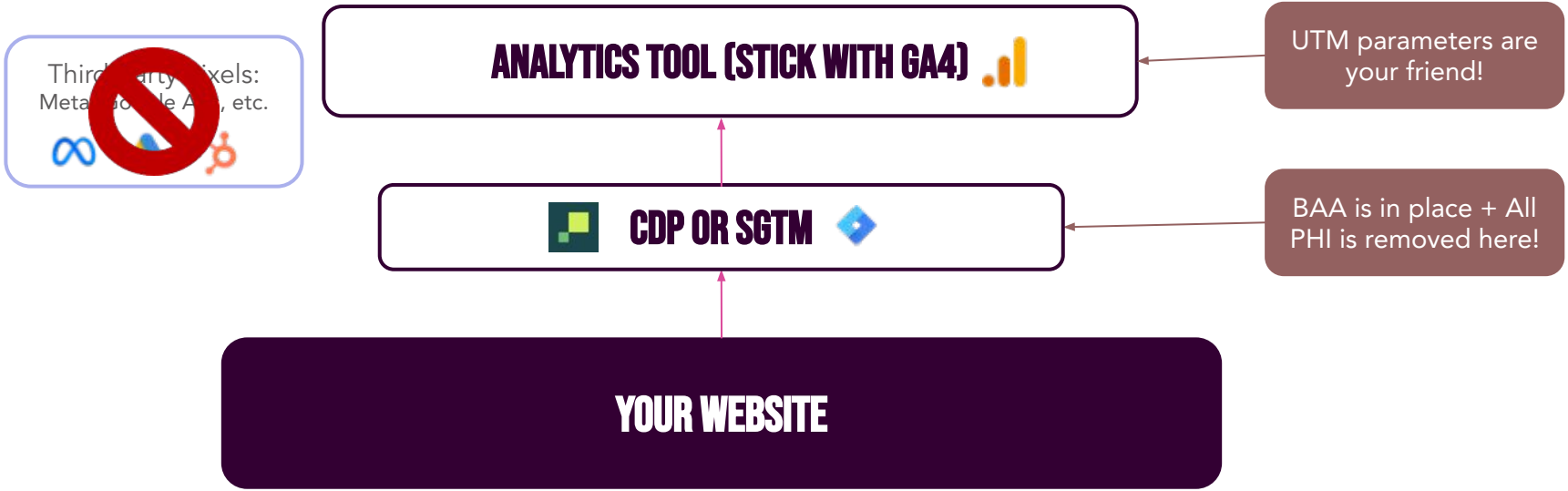
STEP 4: REBUILD ANALYTICS INFRASTRUCTURE FOR THE LONG TERM

Today's (Yesterday's?) Typical Marketing Analytics Structure:



STEP 4: REBUILD ANALYTICS INFRASTRUCTURE FOR THE LONG TERM

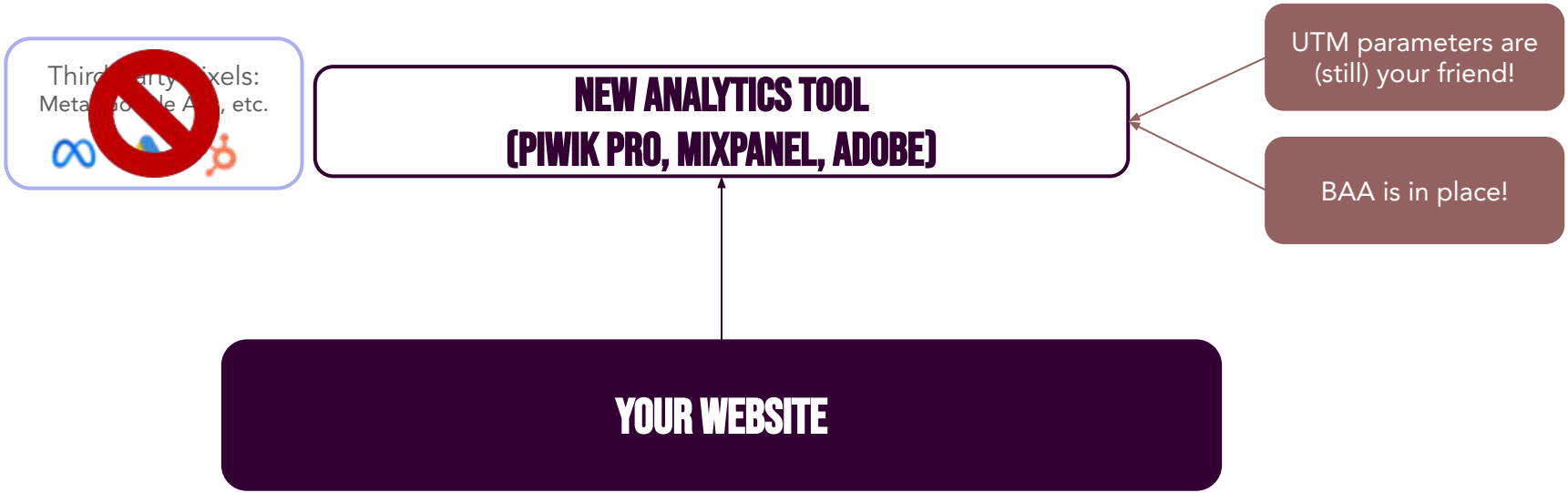
Marketing Analytics Structure for Healthcare – Option 1:



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:



LET'S WEIGH THE OPTIONS

	OPTION 1		OPTION 2
	Server-Side Google Tag Manager (sGTM)	Customer Data Platform (CDP)	New Analytics Tool
Pros	• Less cost • Keep using familiar tools	• Will sign a BAA	• Will sign a BAA
Cons	• Internal team (or agency partner) needs deep analytics knowledge • Time/Cost to implement	• Cost to buy tool (and ongoing cost) • Time/Cost to implement	• Cost to buy tool (and ongoing cost) • Time/Cost to implement
Tool Options	• *Stay with Google Analytics / GTM!*	• Hightouch • FreshPaint • Segment	• Piwik Pro • MixPanel • Adobe

STEP 5: RETHINK YOUR PROCESSES

START AT NO

- Third-party trackers/pixels (Meta, LinkedIn, Google Ads, etc.)
- New tools and technologies

DESIGN FOR THE FUTURE

- First party when possible
- Compliant always

IMPLEMENTING NEW TAGS/TECHNOLOGIES

- Build an approval process
- What information is collected?
- Is is IIHI/PHI?
  - Is there a BAA?

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

SOME WATCH-OUTS

- Call-Tracking Software
- Remarketing & Look-Alike Audiences
- Programmatic
- Email Marketing & CRM tools
- Form Variables into URL Parameters
- Purchased lists uploaded as look-alikes

WHAT TO DO NEXT?

Knowledge (and cross-functional alignment) are power!

Start with asking questions to your internal teams and agency partners.

WE HAVE A HANDOUT!

WE ARE, MARKETING HAPPY.