



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

Jenny Bristow, Hedy & Hopp

# TODAY'S AGENDA

1. How we got here (HIPAA, FTC & State Laws)
2. Three potential paths of action re: Marketing Analytics
3. Digital Marketing tactic watch-outs
4. Extended Q&A (put Qs in the Q&A box)

YES - we will be sharing the deck & recording.

# 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.

## **ANOTHER DISCLAIMER**

This content and presentation is owned by Hedy & Hopp. It may not be distributed or reproduced without express written permission.

**ANOTHER DISCLAIMER**

**ANOTHER ONE**

Agencies - Rising tides lift all ships.

We're here to help and make sure  
patient data is safe.

## DEFINE: COVERED ENTITY

---

Covered entities are defined in the HIPAA rules as

- (1) health plans,
- (2) health care clearinghouses, and
- (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.



# 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?**





# 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 Business Associates Agreement (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.)

# 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.”*

# 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.

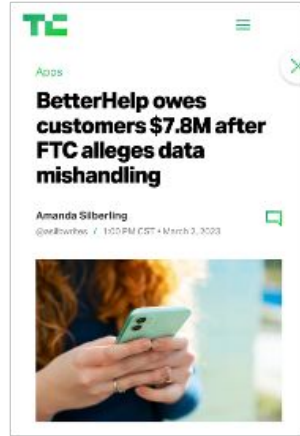
This is legally “consideration” = selling data.

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.



# FTC – IMPACT OF THIS POSITION



**BOTH FINES CAME AS A RESULT OF META PIXELS TO TRACK CONVERSIONS**



# AND THEN, HHS & THE FTC JOINED FORCES



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



# 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



# STATE LAWS – DON'T FORGET



CALIFORNIA JANUARY 1, 2023	CONNECTICUT JULY 1, 2023	VIRGINIA JANUARY 1, 2023	COLORADO JULY 1, 2023
<ul style="list-style-type: none"> <li>allow consumers to opt-out of the sales of personal info</li> <li>honor opt-out preference signals or GPCs</li> <li>allow consumers to limit the processing of sensitive personal info</li> <li>implement data minimization and purposes limitation principles</li> <li>honor CPRA consumer requests</li> <li>provide a privacy notice</li> <li>ensure service providers comply with the law</li> <li>establish a data retention period <i>will likely soon require data brokers to disclose what they collect and allow consumers to direct brokers to delete their personal info</i></li> </ul>	<ul style="list-style-type: none"> <li>allow consumers to opt-out of the processing of sensitive personal info</li> <li>collect and process only the minimum amount of data needed for the processing purpose</li> <li>provide a privacy notice</li> <li>conduct data protection impact assessment where there is a risk <i>will likely soon require to honor opt-out preference signals or GPCs</i></li> </ul>	<ul style="list-style-type: none"> <li>allow consumers to opt-out of the sales of personal info, targeted advertising, and profiling</li> <li>ensure data processing agreements are in place with data processors</li> <li>provide a privacy notice</li> <li>honor consumer requests</li> <li>conduct privacy impact assessment if required for your processing activities</li> </ul>	<ul style="list-style-type: none"> <li>provide consumers to opt-out of the sales of personal info, targeted advertising, and profiling</li> <li>provide a privacy notice</li> <li>conduct data protection impact assessment where there is a risk</li> <li>honor consumer requests <i>will likely soon require to honor opt-out preference signals or GPCs</i></li> </ul>

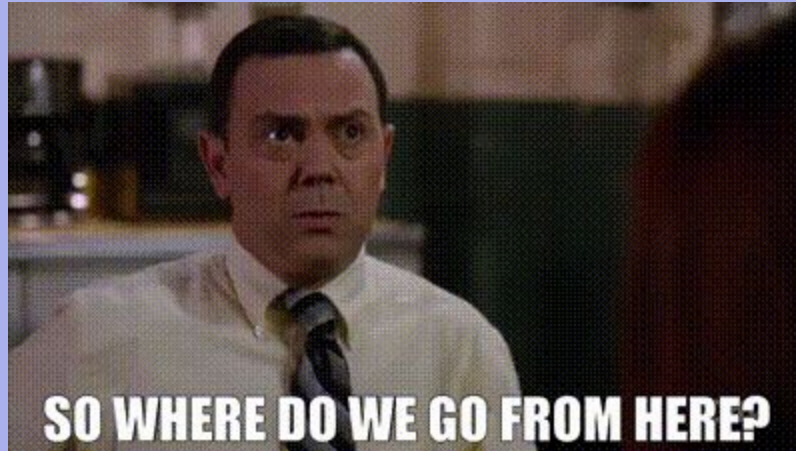
# STATE LAWS – MORE ARE ON THE WAY



UTAH DECEMBER 31, 2023	IOWA JANUARY 1, 2025	INDIANA JANUARY 1, 2026	MONTANA OCTOBER 1, 2024	TENNESSEE JULY 1, 2025
<ul style="list-style-type: none"> <li>honor consumer requests</li> <li>allow consumers to opt-out of the sales of personal info or from targeted advertising</li> <li>have processing agreements in place</li> <li>provide a privacy notice</li> </ul>	<ul style="list-style-type: none"> <li>limit data processing to the specified purposes</li> <li>provide a privacy notice</li> <li>allow consumers to opt-out of the sales of personal info</li> <li>have written contracts with service providers</li> <li>honor consumer requests for access, deletion, portability, opt-out, etc.</li> </ul>	<ul style="list-style-type: none"> <li>allow consumers to opt-out of the sales of personal info</li> <li>obtain explicit consent for the processing of sensitive personal data</li> <li>limit processing to intended purposes</li> <li>honor consumer requests</li> <li>provide a comprehensive privacy notice</li> <li>conduct data impact assessment in the case of targeted advertising</li> </ul>	<ul style="list-style-type: none"> <li>respond to consumer requests</li> <li>allow consumers to opt-out of the sales of personal info</li> <li>recognize universal opt-out mechanisms</li> <li>provide a privacy notice and a privacy policy</li> <li>obtain explicit consent before collecting sensitive data</li> <li>conduct data protection impact assessments for processing sensitive data, selling data, or using data for targeted advertising and/or profiling</li> </ul> <p><i>will likely soon require to honor opt-out preference signals or GPCs</i></p>	<ul style="list-style-type: none"> <li>honor consumer requests to know, access, delete, etc.</li> <li>allow consumers to opt-out of the sales of their data</li> <li>have written contracts with service providers</li> <li>provide a privacy notice and a privacy policy</li> <li>process the data only for the purposes it has been collected for</li> </ul>

# 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.



# 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?

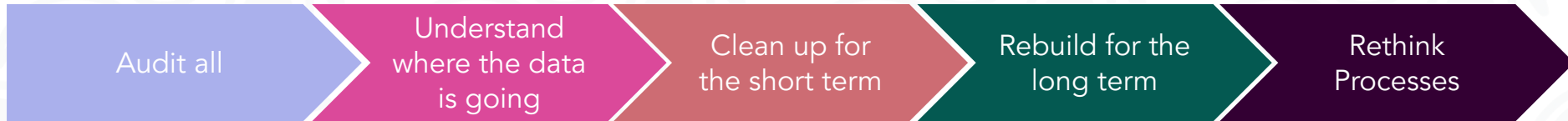
4

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	<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>

**EXAMPLE ONLY!**

Most audits cover 50-75 tools across these four categories

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

Copyright 2023 • Hedy & Hopp • Not for Distribution

## STEP 2: UNDERSTAND WHERE PATIENT DATA IS COLLECTED & SHARED



*Pro Tip - Privacy Policy rewrite content!*

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.	<p>Google Analytics stores 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 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 4 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	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.	<p>PHI/PII is collected through the following ways:</p> <ul style="list-style-type: none"> <li>• What advertisers manually send PHI/PII data when using enhanced conversions</li> <li>• When PHI/PII 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 pages, etc.</li> </ul>

**EXAMPLE ONLY!**

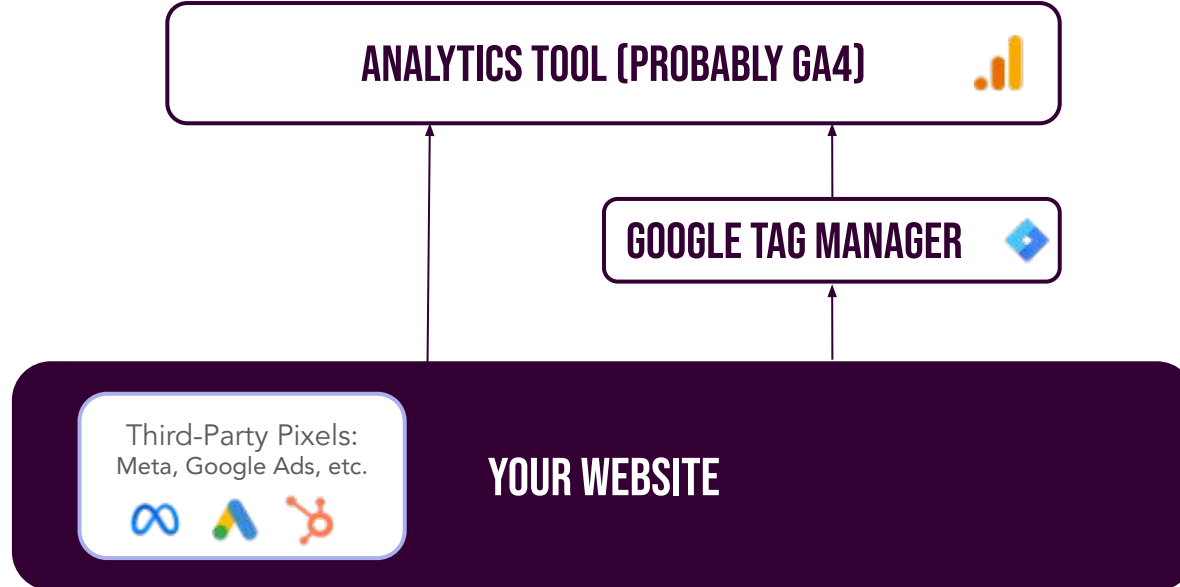
## STEP 3: CLEAN-UP FOR THE SHORT TERM

---

- 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!

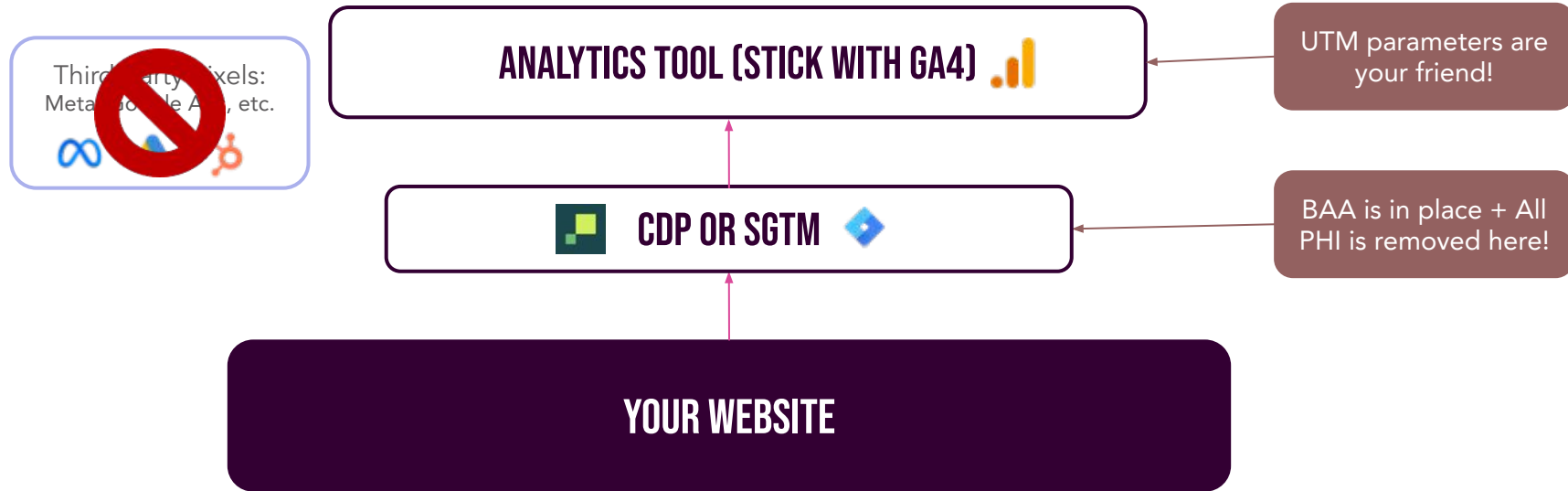
## STEP 4: REBUILD ANALYTICS INFRASTRUCTURE FOR THE LONG TERM

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



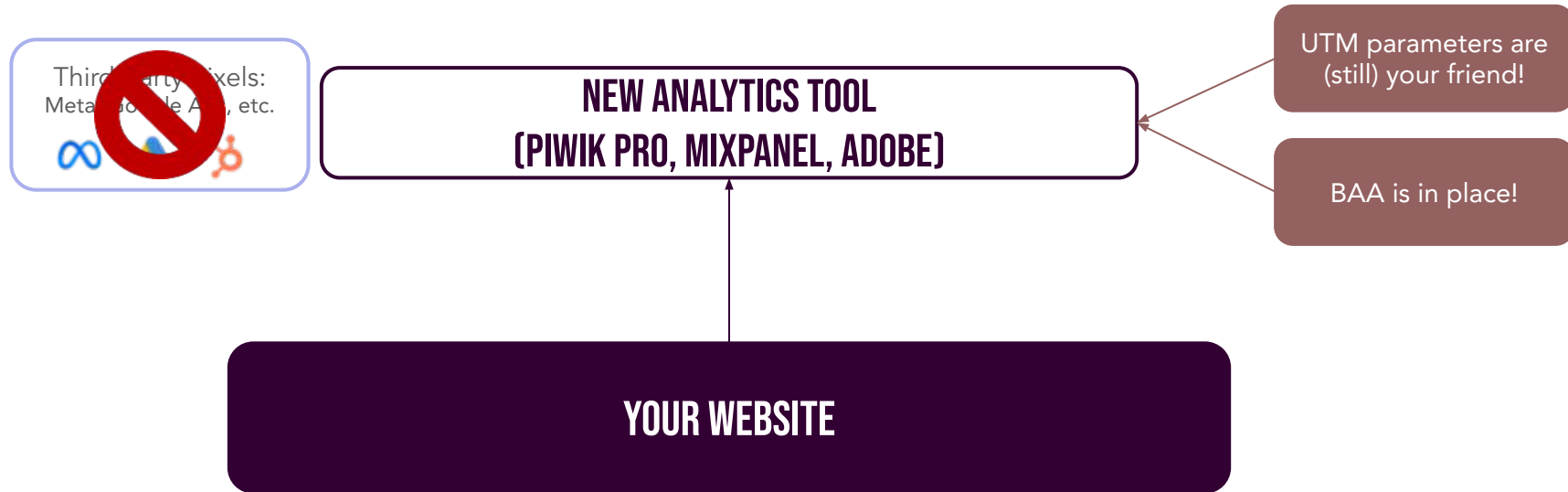
## STEP 4: REBUILD ANALYTICS INFRASTRUCTURE FOR THE LONG TERM

### Marketing Analytics Structure for Healthcare – Option 1:



## 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	<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>	<ul style="list-style-type: none"> <li>Will sign a BAA</li> </ul>
Cons	<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>Cost to buy tool (and ongoing cost)</li> <li>Time/Cost to implement</li> </ul>	<ul style="list-style-type: none"> <li>Cost to buy tool (and ongoing cost)</li> <li>Time/Cost to implement</li> </ul>
Tool Options	<ul style="list-style-type: none"> <li><i>Stay with Google Analytics / GTM!</i></li> </ul>	<ul style="list-style-type: none"> <li>Hightouch</li> <li>FreshPaint</li> <li>Segment</li> </ul>	<ul style="list-style-type: none"> <li>Piwik Pro</li> <li>MixPanel</li> <li>Adobe</li> </ul>



## 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

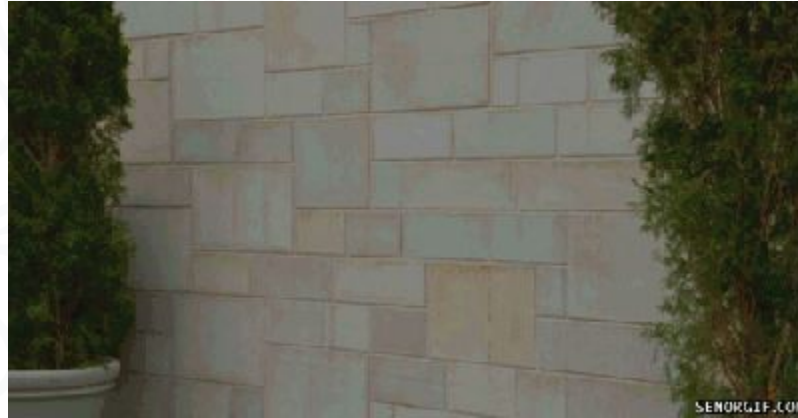
- Build an approval process
- What information is collected?
- Is is IIHI/PHI?
  - Is there a BAA?

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



## SOME MARKETING TACTIC WATCH-OUTS

---



# CALL-TRACKING SOFTWARE QR CODES TEXTING

Q&A from Health & Human Services re: Marketing vs Patient Communication:  
<https://www.hhs.gov/hipaa/for-professionals/fag/marketing/index.html>

# REMARKETING & LOOK-ALIKE AUDIENCES AND PROGRAMMATIC

## PURCHASED LISTS UPLOADED AS LOOK-ALIKES

Remember: IN-PLATFORM is OK.  
Don't feed the beast.

# EMAIL MARKETING & CRM TOOLS

# **EEEEK! WEBSITE DEVELOPMENT CHOICES - FORM VARIABLES INTO URL PARAMETERS**

# **SOCIAL MEDIA MANAGEMENT TOOLS & DM RESPONSE MANAGEMENT**



## 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.**

[jenny@hedyandhopp.com](mailto:jenny@hedyandhopp.com)  
[hedyandhopp.com](https://hedyandhopp.com)