SOCIALCLIMB
HEALTHCARE MARKETING PLATFORM

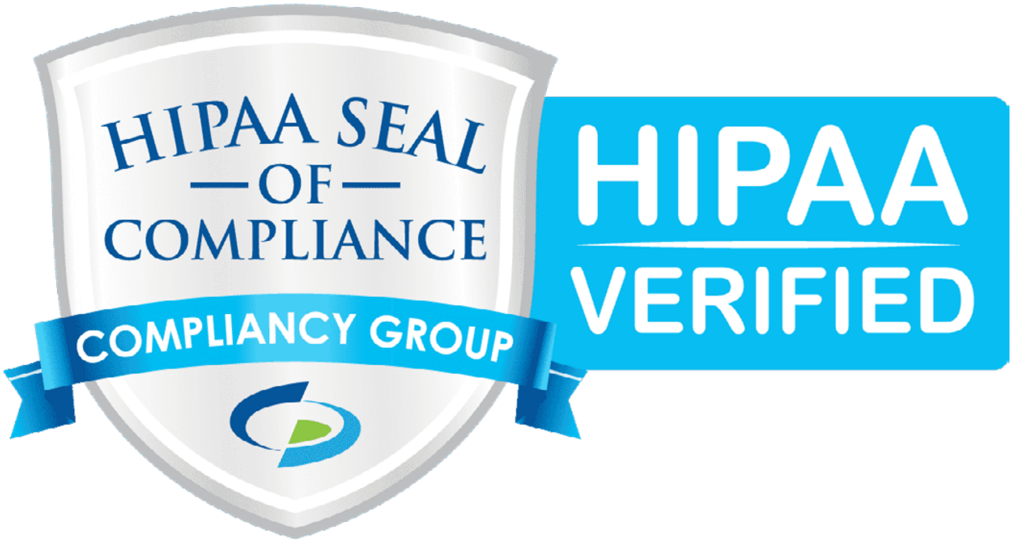
Navigating the Terrain:
Unlocking Healthcare Marketing Success with HIPAA-Compliant Tracking

SocialClimb.com/HIPAA

Table of Contents

“The healthcare industry has become a prime target for hackers. With the threat growing each year, healthcare organizations must be vigilant in their efforts to keep patient information secure.”

**– Marc Haskelson,
President and CEO, Compliancy Group**



Preface

In today's digital age, healthcare practices and organizations are faced with the critical task of ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA). As healthcare marketing evolves and embraces technology, it becomes increasingly challenging to navigate the complex landscape of online advertising, including website analytics, social media, and digital advertising.

Read this eBook if any of these statements apply to you:

- I want to better understand tracking technology putting me at risk
- I have Google Analytics on my website
- I use Google Ads (or other platforms) to target and track patients
- I use Facebook or other social media to market to patients

This eBook will shed light on the potential pitfalls that healthcare practices can encounter when marketing online. As you read, you will 1- explore the nuances of Google Analytics (GA4), 2- learn how many of today's technologies can inadvertently expose sensitive patient data and lead to HIPAA violations, 3- identify remediation strategies to help your healthcare practice or organization harness the power of digital marketing while safeguarding patient privacy and comply with HIPAA regulations.

Use this eBook to navigate popular marketing technologies while maintaining HIPAA compliance.

Elements of HIPAA Compliance in Healthcare Marketing

The U.S. Department of Health and Human Services (HHS) doesn't have specific rules that directly address the use of pixels (scripts) and tracking technologies in the context of protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA). However, HIPAA rules still apply to the use of such technologies in healthcare settings, and organizations must take measures to ensure compliance. Here are some key considerations:

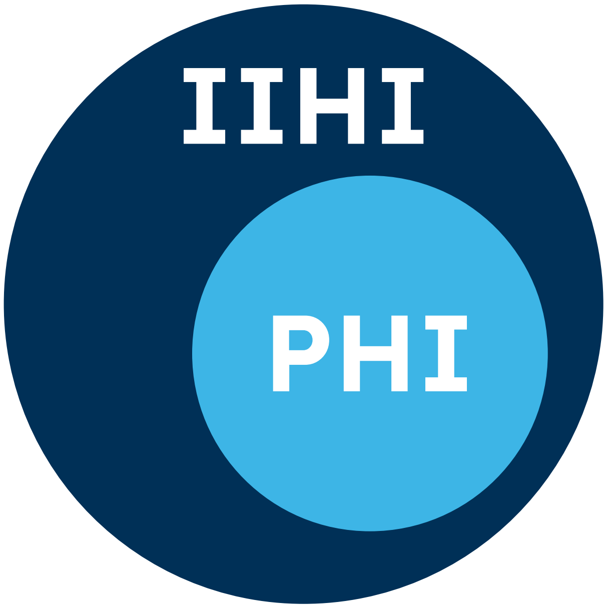
- **PHI Protection:** Pixels, scripts, and tracking technologies can inadvertently collect PHI if not managed properly. HIPAA mandates the protection of PHI, and healthcare organizations must ensure that any data collected through these technologies is properly anonymized and secured.
- **Consent and Transparency:** If pixels, scripts, or tracking mechanisms are used to collect data that could potentially include PHI, obtaining patient consent is essential. Patients should be informed about the data collection, its purpose, and how their information will be used for tracking and marketing.
- **Security and Access Controls:** Implement robust security measures to protect any data collected. This includes encryption, access controls, and regular security assessments to prevent data breaches.
- **Business Associate Agreements (BAAs):** If third-party vendors are involved in the use of tracking technologies and have access to PHI, healthcare organizations must have BAAs in place to ensure that these vendors also comply with HIPAA regulations.
- **Data Retention and Disposal:** Establish clear policies for the retention and disposal of tracking data. Data should not be retained longer than necessary, and it should be securely disposed of when it is no longer needed.
- **HIPAA Training:** Ensure that employees who handle tracking data are trained on HIPAA compliance and understand their responsibilities in safeguarding PHI.

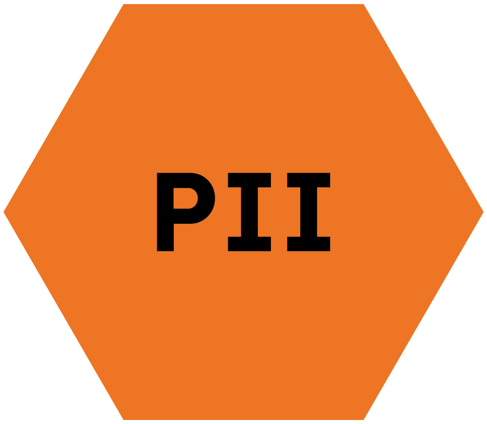
Please note that regulations and guidance related to healthcare data privacy and security may evolve, and it's essential to stay updated with the latest information from HHS and other relevant authorities to ensure compliance with the most current rules and requirements. It's advisable to consult with legal and compliance experts who specialize in healthcare data privacy to navigate the complexities of HIPAA compliance in the context of tracking technologies.

The Difference Between IIHI, PHI and PII

IIHI, PHI, and PII are acronyms related to different types of sensitive information, each with its specific context and usage:

- **IIHI (Individually Identifiable Health Information):** IIHI is a term used in healthcare and is often associated with the Health Insurance Portability and Accountability Act (HIPAA) regulations. IIHI includes information that can be used to identify an individual and is related to that individual's health, treatment, or payment for healthcare services.
- **PHI (Protected Health Information):** PHI is a subset of IIHI, and it encompasses a broader range of health-related information. PHI includes individually identifiable health information but also extends to any information that relates to an individual's past, present, or future physical or mental health, healthcare services, or payment for those services. This data includes (but is not limited to) spoken PHI, PHI written on paper, electronic PHI, and physical or digital images that could identify the subject of health information.
- **PII (Personally Identifiable Information):** PII is a more general term that applies to any information that can be used to identify an individual. It is not specific to healthcare and can include a wide range of personal data, such as names, addresses, social security numbers, phone numbers, email addresses, and more.





In summary, IIHI is health-related information that can identify an individual within the healthcare context, PHI includes a broader set of health-related data under HIPAA regulations, and PII encompasses any information that can identify an individual across various contexts, not limited to healthcare.

What are Tracking Pixels and Tracking Scripts?

Tracking pixels or scripts are tiny pieces of code embedded on websites or in emails. They are used to collect data on user behavior, such as page views, clicks, and conversions, allowing businesses to measure the effectiveness of their online advertising campaigns and optimize their marketing strategies.

Tracking pixels and scripts are both useful marketing tools, but they differ in how they collect data and their purposes:

Tracking Pixels:

- **Image-Based:** Tracking pixels are typically small, invisible, and transparent images embedded on web pages or in emails. They are loaded as part of the page's content.
- **Data Collection:** When a user opens a webpage or email containing a tracking pixel, the pixel sends a request to the server hosting the pixel image. The server logs this data, which can include details on user interactions and behaviors.
- **Purpose:** Tracking pixels are commonly used for various purposes, such as monitoring website traffic, measuring email open rates, and tracking conversions in digital advertising. They are often used for basic analytics and monitoring user engagement.

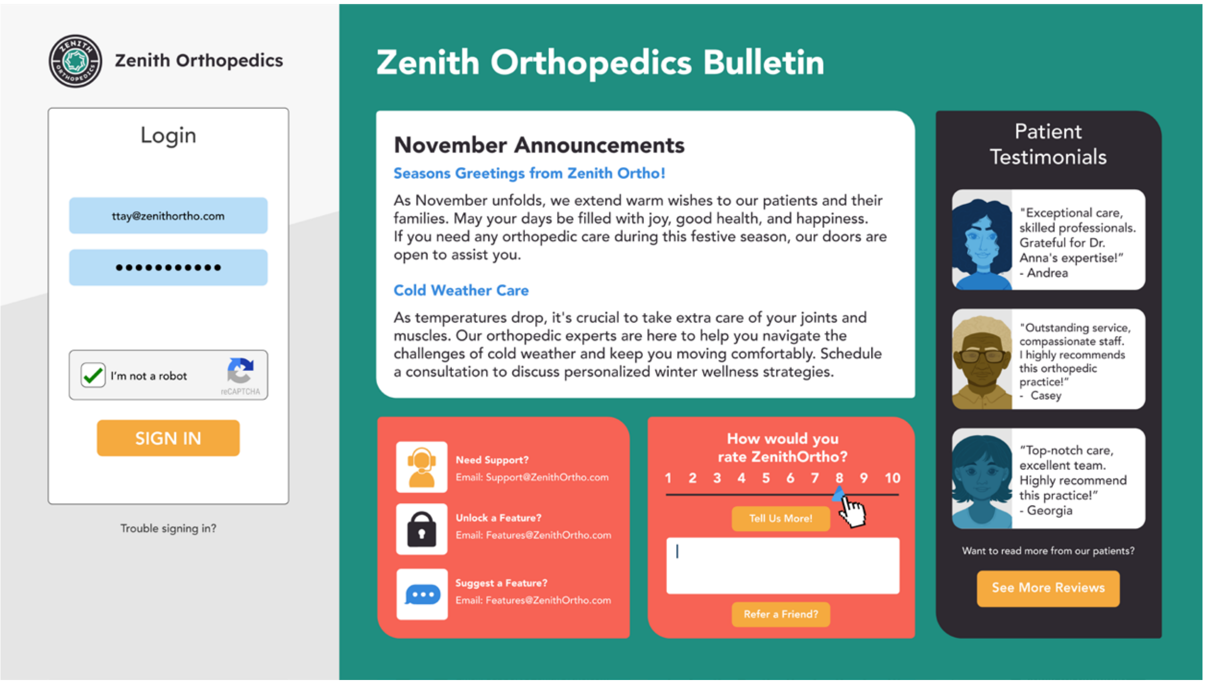
Tracking Scripts:

- **JavaScript Code: Tracking scripts are snippets of JavaScript code embedded within webpages. They are executed by the user's browser when the webpage loads.**
- **Data Collection**: Tracking scripts can collect a wide range of data, including user interactions, mouse movements, clicks, form submissions, and more. They can track user behavior in real-time and send this data to external servers for analysis.
- **Purpose:** Tracking scripts are versatile and can be used for advanced analytics, user experience optimization, A/B testing, and tracking user journeys on websites. They are often employed for in-depth data analysis and personalization of user experiences.

Facebook/Meta

The Facebook pixel (script) is a piece of code that you add to your website. It serves several essential functions for businesses and marketers advertising on Facebook:

What are Tracking Pixels and Tracking Scripts?



Zenith Orthopedics Bulletin

November Announcements

Seasons Greetings from Zenith Ortho!

As November unfolds, we extend warm wishes to our patients and their families. May your days be filled with joy, good health, and happiness. If you need any orthopedic care during this festive season, our doors are open to assist you.

Cold Weather Care

As temperatures drop, it's crucial to take extra care of your joints and muscles. Our orthopedic experts are here to help you navigate the challenges of cold weather and keep you moving comfortably. Schedule a consultation to discuss personalized winter wellness strategies.

Need Support?
Email: Support@ZenithOrtho.com

Unlock a Feature?
Email: Features@ZenithOrtho.com

Suggest a Feature?
Email: Features@ZenithOrtho.com

How would you rate ZenithOrtho?

Patient Testimonials

"Exceptional care, skilled professionals. Grateful for Dr. Anna's expertise!"
- Andrea

"Outstanding service, compassionate staff. I highly recommends this orthopedic practice!"
- Casey

"Top-notch care, excellent team. Highly recommend this practice!"
- Georgia

Want to read more from our patients?

- **Conversion Tracking:** The Facebook script helps you track specific actions that users take on your website after clicking on a Facebook ad. This could include making a purchase, scheduling an appointment, paying a bill, signing up for a newsletter, or filling out a contact form. By tracking these conversions, you can measure the effectiveness of your Facebook advertising campaigns.
- **Audience Building:** The pixel collects data on your website visitors, allowing you to create custom audiences based on their behavior. For example, you can create an audience of people who visited a specific procedure page but didn't schedule an appointment or make a purchase. You can then use this audience for retargeting ads to encourage them to complete the purchase.
- **Optimizing Ad Delivery:** Facebook uses pixel data to optimize the delivery of your ads. This pixel helps Facebook refine your ads and show them to people who are more likely to take the desired action, such as making a purchase or scheduling an appointment, based on their past behavior.
- **Attribution:** The Facebook pixel provides insights into how different interactions with your ads contribute to conversions. This helps you understand the patient journey and make informed decisions about your marketing strategy.

Need help? SocialClimb will assess your online HIPAA-compliance.
Contact your CSM or visit us at marketing.socialclimb.com/hipaa-compliance

Google Analytics

Marketers across various industries often employ Facebook tracking pixels on their websites to gain insights into user behavior. These tracking pixels enable them to collect data on visitor interactions, such as page views and form submissions. This data-driven approach empowers marketers to make informed decisions, refine their advertising strategies, and allocate resources efficiently.

Google Analytics

Google Analytics 4, or GA4, is a tool that helps website and app owners understand how people use their website. It provides information about website visitors: visitor counts, website entry points, webpage visits, actions taken, etc. In simple terms, GA4 gives you data to see how well your website is doing and helps you make it better to attract and serve your audience. This robust tool offers comprehensive insights into how users interact with your websites, including data on user demographics, traffic sources, and browsing behavior. User metrics combined with an individual's IP address creates PHI and HIPAA non-compliance.

Placing Google Analytics or any tracking scripts on patient login screens or portals in a healthcare setting raises significant HIPAA-compliance concerns. These screens often contain protected health information (PHI) or individually identifiable health information (IIHI), which must be safeguarded under HIPAA regulations. Google Analytics and similar tracking tools can inadvertently collect and transmit this sensitive data, potentially leading to HIPAA violations and legal consequences. Moreover, patient login screens and portals serve as gateways to confidential medical records, making them high-risk areas for data breaches. To ensure HIPAA compliance, healthcare organizations should carefully assess the necessity of tracking on such pages, implement robust security measures, and consider alternatives for tracking that do not compromise patient privacy or violate HIPAA regulations.

Google Ads

Healthcare marketers often use Google Ads tracking pixels and scripts to tailor content, set up audiences, and track user movements. This approach poses unique challenges related to HIPAA compliance. Healthcare organizations must be especially cautious when implementing tracking mechanisms as they handle sensitive patient data. Ensuring that Google Ads tracking scripts or pixels do not inadvertently collect or expose protected health information (PHI) is crucial to maintain HIPAA compliance. Healthcare marketers must strike a balance between effective advertising and safeguarding patient privacy. **Custom audiences and tailored content are valuable for reaching the right patients with relevant information, but careful consideration for patient data must be taken.**

Other Advertising

Other Advertising

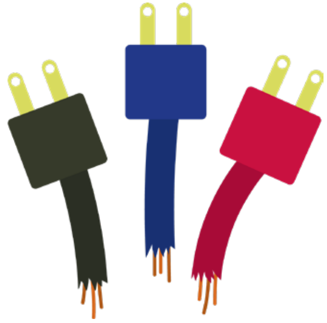
Various digital marketing activities, especially those using tracking scripts, can potentially put healthcare organizations at risk of non-compliance with HIPAA regulations. For instance, when utilizing platforms like Microsoft Bing Ads, LinkedIn, Twitter, TikTok, and others, healthcare marketers may inadvertently collect, combine, or expose patient information.

Examples include using tracking scripts to target ads based on users' online behavior, which might include health-related searches or interactions with medical content. While such targeting can be effective, it can also risk revealing patient interests or conditions. Moreover, retargeting campaigns that rely on tracking scripts may display healthcare-related ads to users who have previously visited a healthcare provider's website, potentially disclosing the fact that they sought specific medical services.

These scenarios emphasize the need for healthcare organizations to exercise caution when employing tracking scripts on digital marketing platforms to balance the benefits of personalized marketing with strict adherence to HIPAA compliance standards.

Need help? SocialClimb will assess your online HIPAA-compliance.
Contact your CSM or visit us at marketing.socialclimb.com/hipaa-compliance

WordPress, Plugins, and HIPAA-Compliance



WordPress websites often rely on a wide range of plugins to enhance functionality and features. Plugins are add-on software components that extend the functionality of websites, allowing users to easily integrate new features and customize their sites without altering the core code.

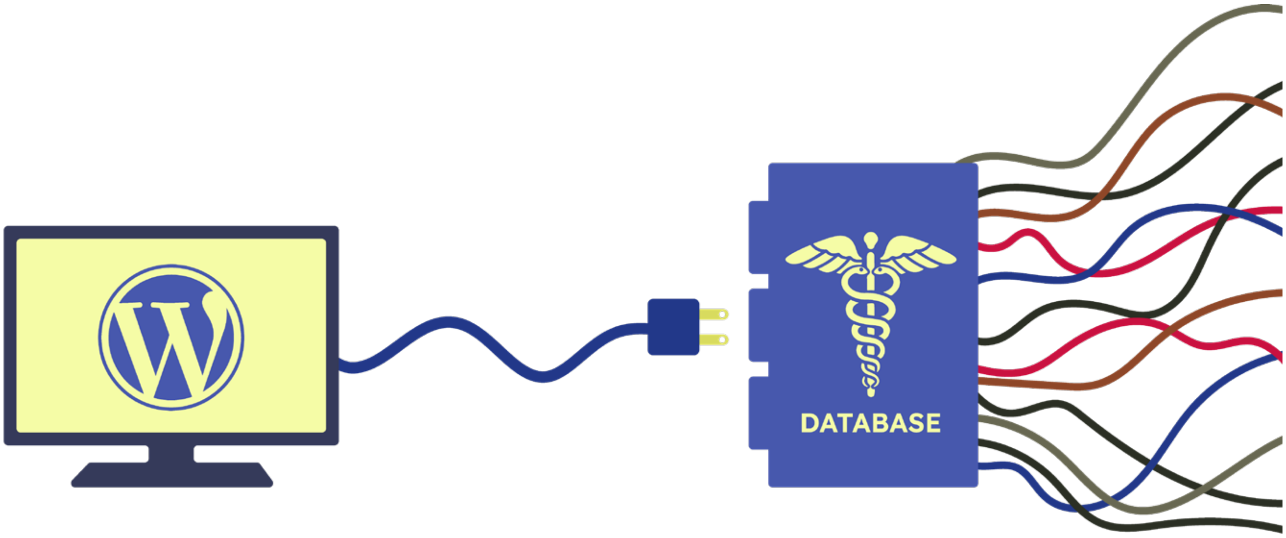
However, integrating and managing WordPress plugins while maintaining compliance can present HIPAA-Compliancy challenges:

- **Plugin Security:** Many WordPress plugins are developed by third-party vendors, and their security measures may not always align with HIPAA requirements. Using non-HIPAA-compliant plugins can introduce vulnerabilities into your website, potentially leading to compliance violations.
- **PHI Handling:** Some plugins may inadvertently store or transmit PHI without proper encryption or access controls. Ensuring that all plugins used on a healthcare website are HIPAA-compliant is imperative.
- **Plugin Updates:** Plugins require regular updates to patch security vulnerabilities and maintain functionality. However, not all plugin developers prioritize security updates, leaving WordPress websites at risk of non-compliance if plugins are not promptly updated and monitored for potential issues.
- **Limited Plugin Oversight:** WordPress websites can use numerous plugins simultaneously, and each one may handle different aspects of the site. This can make it challenging to monitor and control the handling of PHI across all plugins, potentially leading to data breaches and HIPAA violations.
- **Lack of Audit Trails:** HIPAA compliance requires detailed audit trails to track access to PHI. While some plugins offer basic logging capabilities, they may not provide the comprehensive audit trails required for HIPAA compliance. Integrating third-party auditing solutions or custom development may be necessary.

WordPress, Plugins, and HIPAA-Compliance

- **Plugin Compatibility:** Ensuring that all plugins used on a WordPress healthcare website are compatible with each other and with the specific compliance requirements of HIPAA can be a complex task. Incompatibilities can lead to data inconsistencies and security vulnerabilities.
- **Vendor Support and BAAs:** If a plugin vendor is involved in the management of PHI, HIPAA mandates the establishment of Business Associate Agreements (BAAs). Securing BAAs with multiple plugin vendors can be logistically challenging, and not all vendors may be willing to enter into such agreements.
- **Plugin Evaluation:** Careful evaluation and testing of plugins for their suitability for healthcare and HIPAA compliance is essential. This process requires a deep understanding of both WordPress and HIPAA regulations, making it a time-consuming endeavor.

While WordPress plugins can significantly enhance the functionality and capabilities of a healthcare website, they also present unique challenges when it comes to achieving and maintaining HIPAA compliance. Healthcare organizations using WordPress should exercise caution when selecting, configuring, and managing plugins to ensure that they align with HIPAA requirements and do not compromise the security of patient data. Regular security assessments and audits of plugins are essential for maintaining compliance in a dynamic digital environment.



Why Now?

Tracking scripts, such as the Facebook script, have become a bigger concern for healthcare practices compared to a few years ago due to several factors:

- **Increased Tracking Detail:** The evolution from tracking pixels to tracking scripts has marked a significant transformation in the world of digital analytics and user behavior tracking. While tracking pixels have been widely used since the early days of the internet, the transition to tracking scripts began gaining momentum around the mid-2000s. This shift allowed for a more sophisticated approach to data collection and analysis. With tracking scripts, such as JavaScript-based solutions, the level of detail and granularity in data increased substantially. Unlike pixels, scripts could capture real-time user interactions, such as mouse movements, clicks, form submissions, and even the time spent on specific page elements. This transition, driven by the need for more precise insights into user behavior and website performance, enabled businesses to optimize user experiences, conduct A/B testing, and gain deeper insights into the intricacies of online user journeys. As a result, tracking scripts have become the foundation of modern web analytics, providing non-healthcare businesses with the tools needed to refine their online strategies and enhance user engagement.

  The increased tracking details that tracking scripts contain, raise HIPAA concerns when used in healthcare settings, as they may inadvertently capture and expose protected health information (PHI), necessitating careful implementation and data security measures to ensure compliance with HIPAA regulations.
- **Increased Digital Presence:** Healthcare practices have expanded their online presence significantly in recent years. They now rely on websites, social media, and digital advertising to attract and engage patients. This increased digital activity means more data is being collected, making the use of pixels more prevalent.
- **Data Privacy Awareness:** There's a growing awareness of data privacy concerns among patients and the general public. High-profile data breaches and increased media coverage of privacy issues have made people more cautious about how their personal information is collected and used.
- **HIPAA Compliance Litigation:** The Department of Health and Human Services (HHS) has recently increased its fines for HIPAA (Health Insurance Portability and Accountability Act) compliance violations, signaling a stricter enforcement approach.

Why Now?

- **3rd Party Cookies**:** The depreciation of 3rd party internet cookies has prompted a significant shift in the digital marketing landscape. As these cookies are phased out, marketers are reevaluating their strategies for tracking user interactions and delivering personalized content. This transition has paved the way for alternative methods, such as 1st party data collection, contextual advertising, and privacy-centric tracking technologies. Marketers are focusing more on building direct relationships with their audiences and relying on data obtained through user consent and engagement on their own platforms. While the shift away from 3rd party cookies presents challenges, it also promotes a more privacy-conscious approach, emphasizing user consent, data protection, and transparent communication in the digital marketing realm.

***1st Party and 3rd Party Cookies - The difference between 1st party and 3rd party cookies lies in their origin and purpose. 1st party cookies are set by the website the user is currently visiting, and they are primarily used to enhance the user experience by remembering user preferences and login information. These cookies are considered more trustworthy and privacy-friendly, as they are directly associated with the website the user is interacting with. In contrast, 3rd party cookies are set by domains other than the one the user is visiting and are often used for tracking and advertising purposes across multiple websites. While they enable personalized advertising and analytics, 3rd party cookies have raised privacy concerns and have been restricted by many web browsers and privacy regulations due to their potential for intrusive tracking across the internet.*

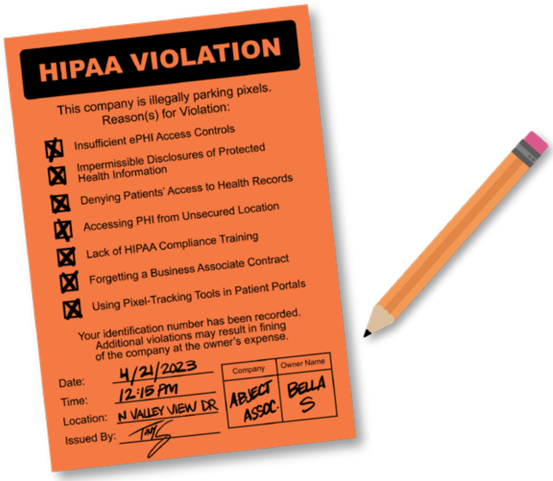
- **Cybersecurity Threats:** The healthcare industry is a prime target for cyberattacks. Pixels and tracking mechanisms, if not adequately secured, can become entry points for hackers to access sensitive patient data..

As a result of these factors, healthcare practices are now more cautious about implementing pixels and other tracking tools. They must take measures to ensure that data collected through these mechanisms is properly anonymized, secured, and used in compliance with privacy regulations like HIPAA. Additionally, they need to be transparent with patients about data collection practices and obtain informed consent when necessary. This increased concern reflects the evolving landscape of data privacy and security in healthcare.

Putting Your Practice at Risk

As stated in the preceding sections, healthcare practices and organizations must prioritize patient privacy and comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations when implementing tracking mechanisms like the Facebook pixel and Google Analytics 4. Here's how these tools can potentially pose HIPAA compliance risks:

- **Data Collection:** Both the Facebook pixel and GA4 collect user data, including IP addresses and user behavior. While this data may seem innocuous, IP addresses* combined with some types of website browsing data become PHI. For example, if an individual visits your website in search of specific information on knee pain, one can assume that IP Address has specific knee related issues and therefore becomes PHI.
- **Data Transmission:** PHI transmission is also highly regulated and must be sent using secure and encrypted methods. A BAA also must be in place with the recipient of PHI data.
- **Custom Audiences:** Marketers often use tracking tools (Google Analytics, Facebook, Google Ads) to create custom audiences for retargeting. If the tracking data allows for the identification of individuals who have visited healthcare-related pages on the website, it could potentially reveal sensitive health information and violate HIPAA.
- **List Uploads:** Uploading patient lists for marketing campaigns, targeting, or creating look-alike audiences within healthcare organizations carries significant HIPAA compliance risk. Healthcare organizations must have an existing Business Associate Agreements (BAAs) with third-party vendors and advertising platforms before these platforms can handle g PHI. Additionally, it is unlawful to use specifics of healthcare data to identify, target, or communicate with prospective patients.



HIPAA VIOLATION

This company is illegally parking pixels.
Reason(s) for Violation:

☒ Insufficient ePHI Access Controls
☒ Impermissible Disclosures of Protected Health Information
☒ Denying Patients' Access to Health Records
☒ Accessing PHI from Unsecured Location
☒ Lack of HIPAA Compliance Training
☒ Forgetting a Business Associate Contract
☒ Using Pixel-Tracking Tools in Patient Portals

Your identification number has been recorded.
Additional violations may result in fining
of the company at the owner's expense.

Date: 4/21/2023
Time: 12:15 PM
Location: N VALLEY VIEW DR
Issued By:

Company	Owner Name
ABJECT ASSOC.	BELLA S

Need help? SocialClimb will assess your online HIPAA-compliance.
Contact your CSM or visit us at marketing.socialclimb.com/hipaa-compliance

Putting Your Practice at Risk

- **Data Security:** Storing tracking data securely is crucial to preventing data breaches. If there's a security breach and PHI is exposed, it could lead to HIPAA violations and penalties.
- **Website Forms:** Collecting data through a lead form may not be HIPAA compliant because it often involves the collection of protected health information (PHI). When data is collected through lead forms without the necessary consent and security measures, it poses a risk of unauthorized access, exposure of sensitive information, risky data storage, and potential violations of HIPAA rules.

**IP Addresses - An IP address, which stands for "Internet Protocol address," is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two primary functions:*

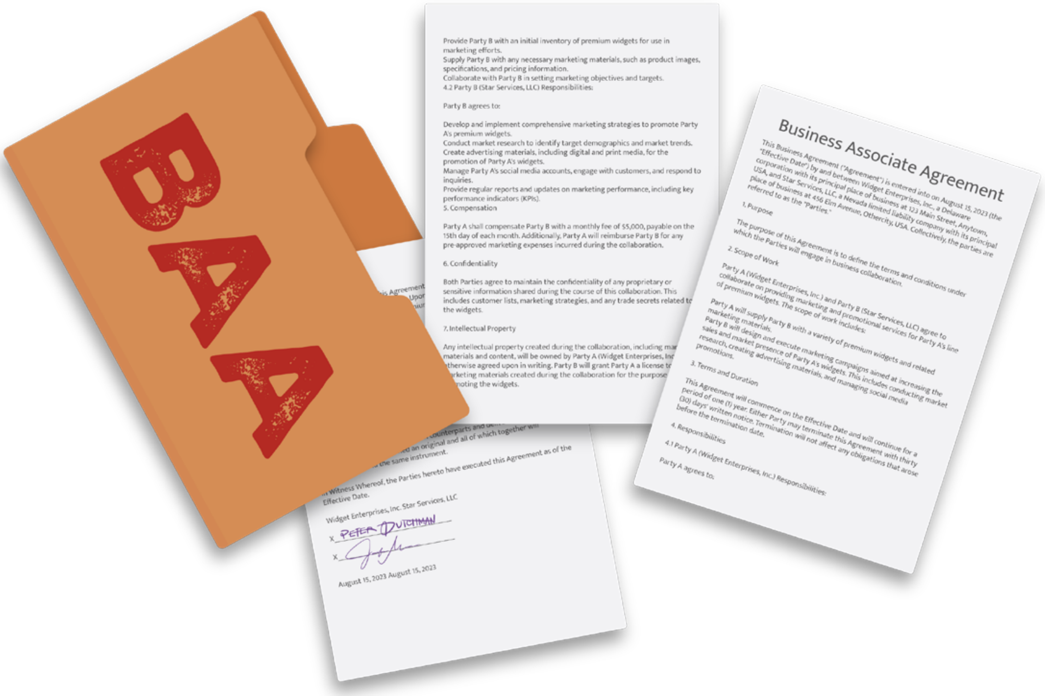
- ***Device Identification: An IP address acts like a digital address for devices on a network. It helps identify a specific device, whether it's a computer, smartphone, server, or any other device connected to the internet. This identification is crucial for data routing and communication.***
- ***Location Address: IP addresses also provide information about the approximate geographical location of a device. While they don't pinpoint an exact physical address, they can often reveal the general region or city where a device is located. This location information is used for various purposes, including content delivery and network optimization.***

Digital Marketing While Maintaining HIPAA Compliance

In summary, while tracking mechanisms like the Facebook script and GA4 can provide valuable insights into healthcare marketing, healthcare practices must be cautious and take appropriate measures to protect patient privacy and maintain HIPAA compliance when implementing these tools.

Yes, it is still possible to track your marketing efforts in the healthcare industry while adhering to the regulations about HIPAA compliance and digital marketing. However, it requires a careful approach. Here are some key strategies to achieve this:

- **Business Associate Agreement (BAA):** A BAA in healthcare is a legally binding contract that outlines the responsibilities and obligations of third-party entities (partners or vendors) when handling Protected Health Information (PHI) on behalf of a covered entity, such as a healthcare provider or insurer. It is crucial to have third-party associations sign a BAA because it ensures that these entities are committed to maintaining the confidentiality and security of PHI, as required by the Health Insurance Portability and Accountability Act (HIPAA). This agreement helps safeguard patient privacy and data integrity by holding all parties accountable for complying with HIPAA regulations and establishes clear guidelines for the secure handling, storage, and transmission of PHI. *All partners or vendors for your practice should have current BAA in place. Note: Facebook, Google, Bing, and other advertising platforms do not typically sign BAAs with healthcare entities.*

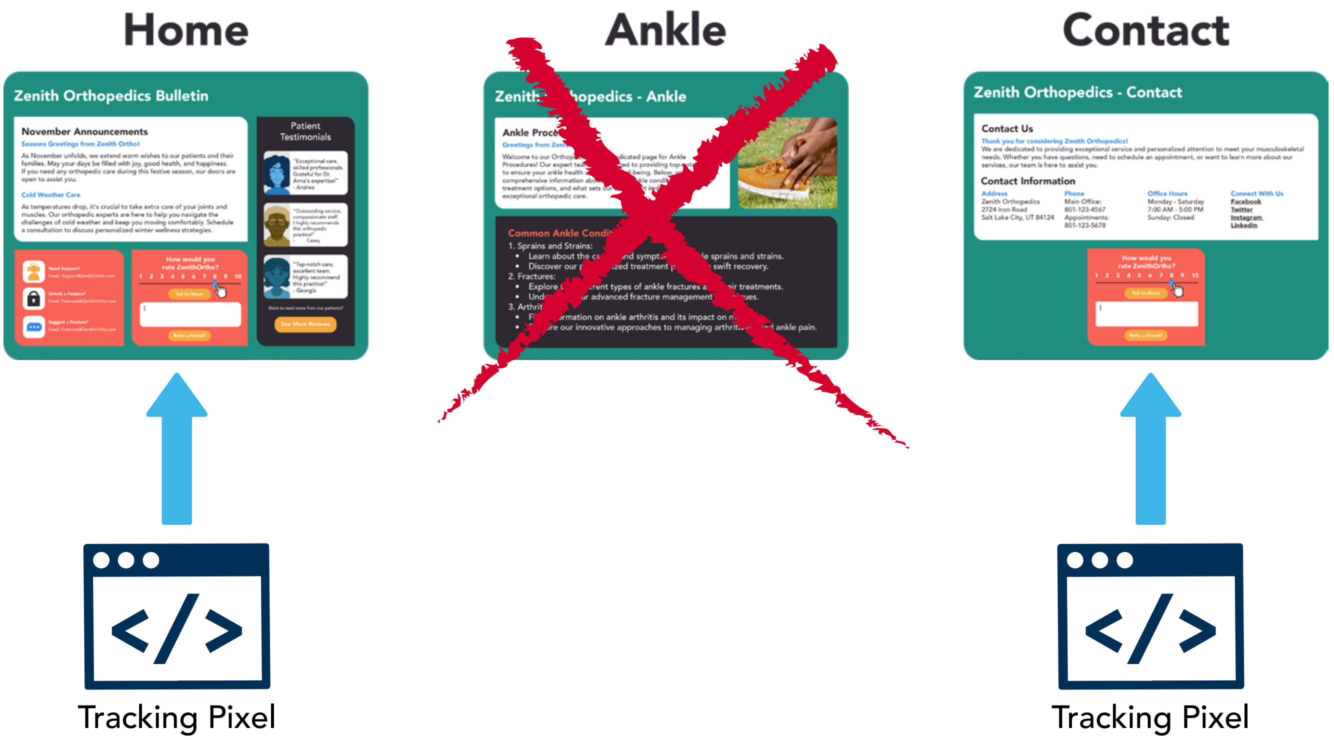


Digital Marketing While Maintaining HIPAA Compliance

Search History + IP = PHI

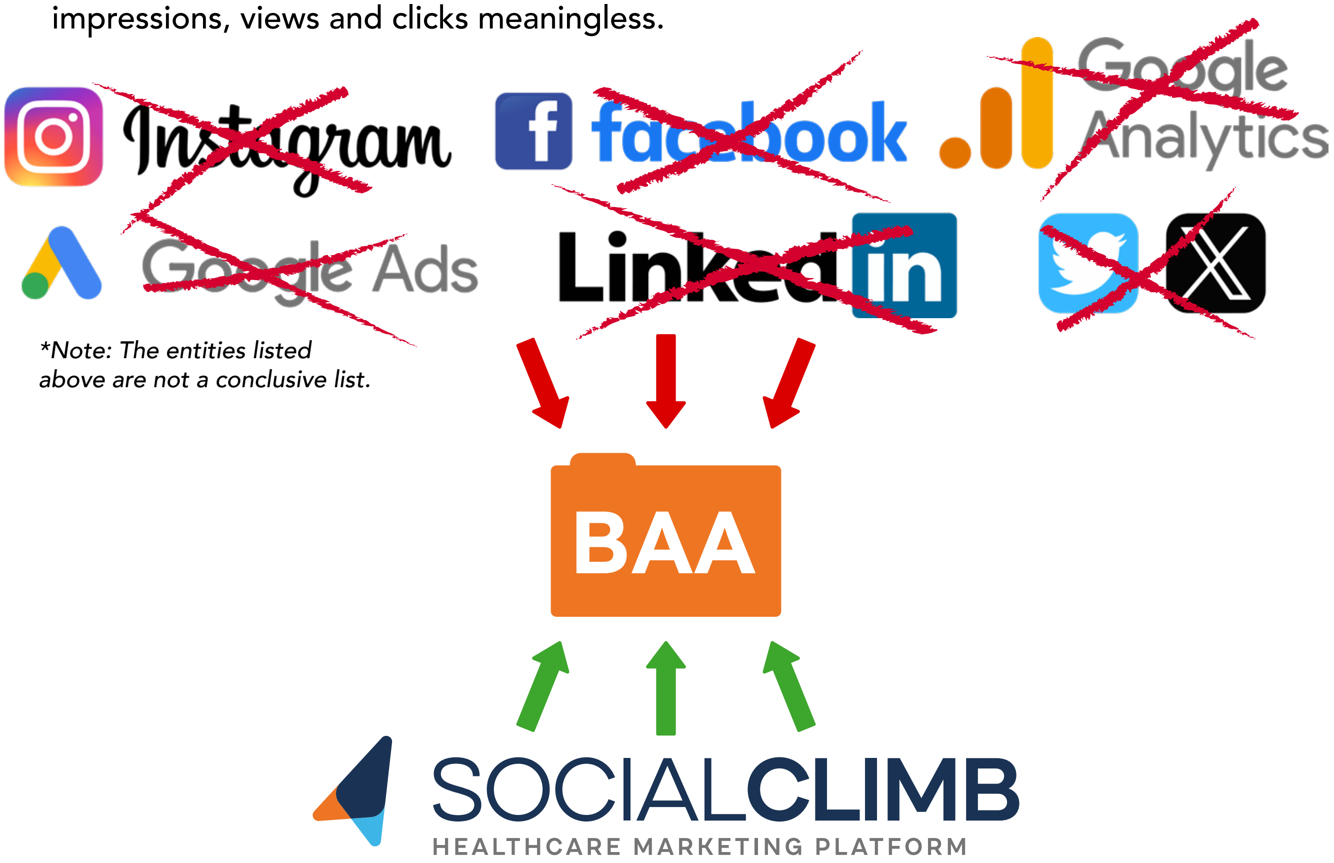
- **Place Tracking Scripts Selectively:** Placing Google and Facebook scripts on your website pages that do not contain health-related data is still a risky option. In non-healthcare industries, tracking scripts are placed in a site-wide manner using tools that place the code across every page. A common thought in healthcare is to remove the tracking scripts from care-specific pages and patient portals for HIPAA compliance. While this might seem like a HIPAA-compliant alternative, in reality PHI inferences can still be made on patient entry and exit pages in GA4 using this method.

Google Analytics


Home
Zenith Orthopedics Bulletin
Ankle
Zenith Orthopedics - Ankle
Contact
Zenith Orthopedics - Contact
Tracking Pixel
Tracking Pixel

Digital Marketing While Maintaining HIPAA Compliance

- **Track Marketing Data Differently:** Although Facebook and Google tracking scripts can be helpful in tailoring your marketing strategy, there are other ways to track and report on marketing efforts. HIPAA-compliant vendors, with a standing BAA, often integrate with your practice management (PM) system and provide you with quantifiable marketing results tracking data. This data allows you to attribute marketing efforts to real patients acquired through your marketing efforts and better understand the efficacy of marketing programs. SocialClimb's Healthcare Marketing Platform allows you to measure your marketing by attaching patient conversions to distinct marketing campaigns. This data allows you to allocate your resources to marketing efforts that produce results (actual patient appointments) – rendering vanity metrics like impressions, views and clicks meaningless.



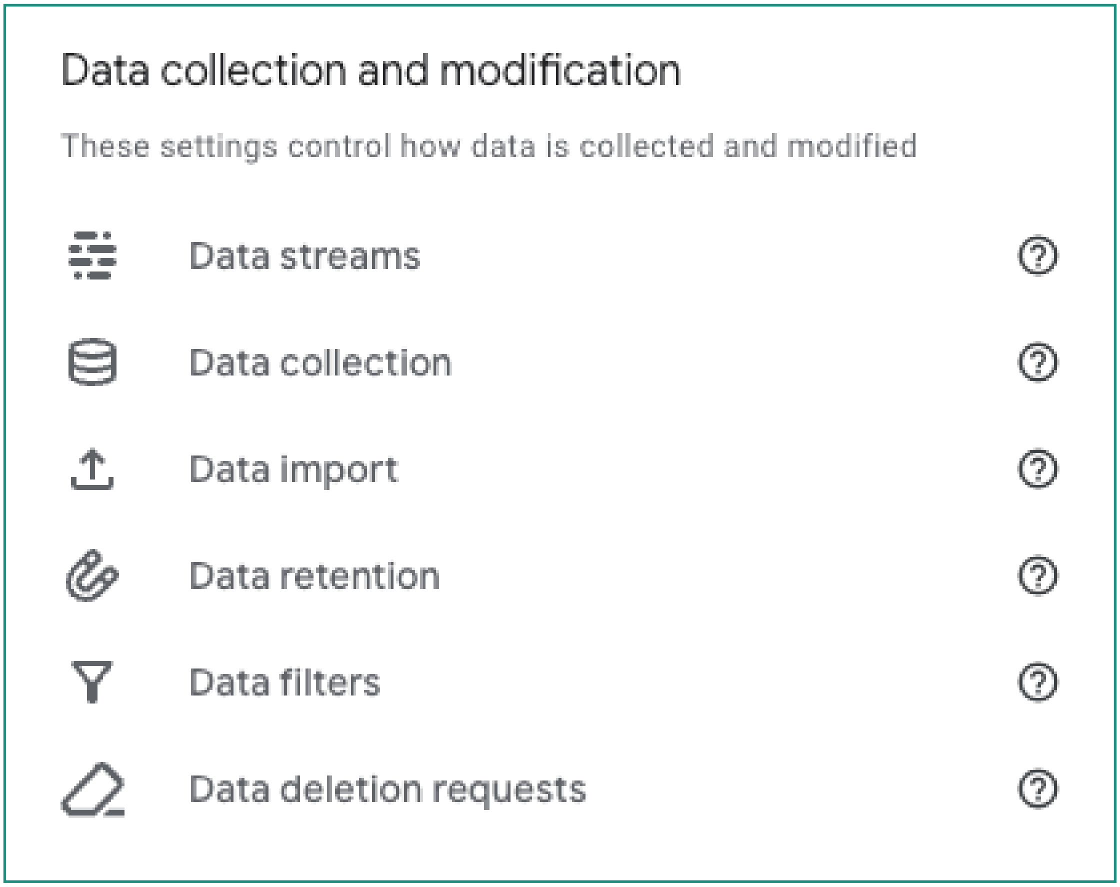
**Note: The entities listed above are not a conclusive list.*

- **Data Anonymization:** Like street addresses, IP addresses pinpoint an individual's location and create ½ of the PHI equation. Unlike previous versions of Google Analytics, GA4 is able to mask a portion of the IP address to hide the location portion of the IP number. While this may seem like the solution to website analytics conundrum, Google still transmits and matches IP data in a temporary memory before it is anonymized. The transmission of PHI data leaves some healthcare entities feeling uneasy as it is not fully HIPAA-compliant. Facebook and other ad platforms typically do not offer the data anonymization feature found in the newest version of Google Analytics.

Digital Marketing While Maintaining HIPAA Compliance

Data Anonymizing features in Google Analytics can be turned on by following the steps below:

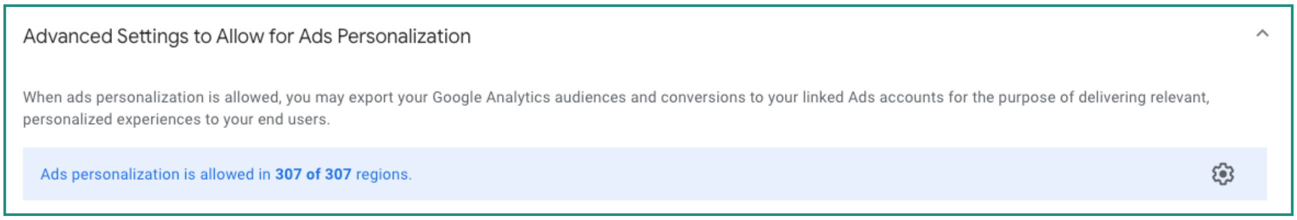
- **Go to the Admin section in GA 4 and then /Data Settings/Data Collection.**



Data collection and modification

These settings control how data is collected and modified

- **Select the gear icon in the Advanced Settings to Allow for Ads Personalization.**



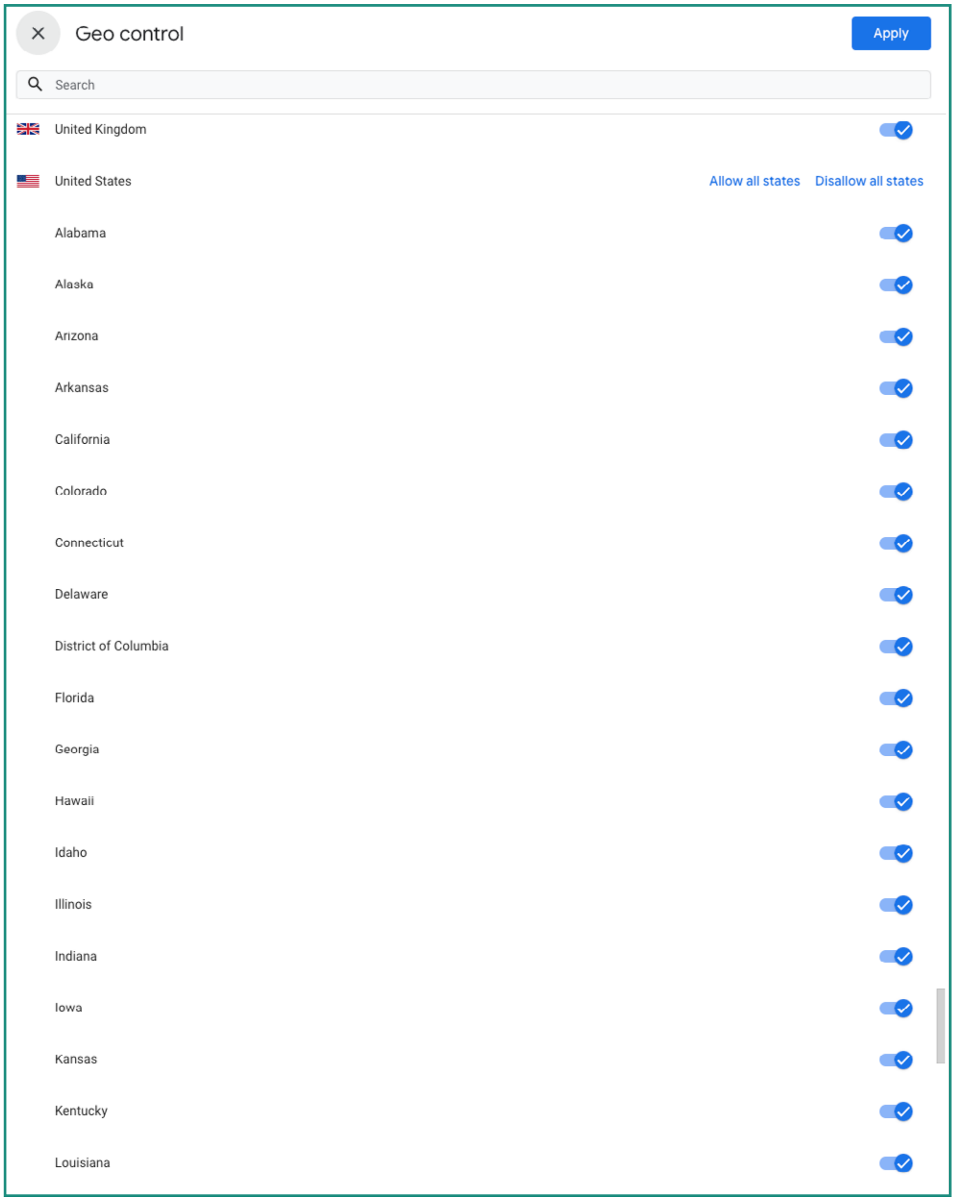
Advanced Settings to Allow for Ads Personalization

When ads personalization is allowed, you may export your Google Analytics audiences and conversions to your linked Ads accounts for the purpose of delivering relevant, personalized experiences to your end users.

Ads personalization is allowed in **307 of 307** regions.

Digital Marketing While Maintaining HIPAA Compliance

- Scroll to the bottom where you see the United States (other countries if necessary)
- Select Disallow all States. *Keep in mind that potential patients from various states may access and interact with your website.



United Kingdom ✓

United States — Allow all states | Disallow all states

Alabama ✓

Alaska ✓

Arizona ✓

Arkansas ✓

California ✓

Colorado ✓

Connecticut ✓

Delaware ✓

District of Columbia ✓

Florida ✓

Georgia ✓

Hawaii ✓

Idaho ✓

Illinois ✓

Indiana ✓

Iowa ✓

Kansas ✓

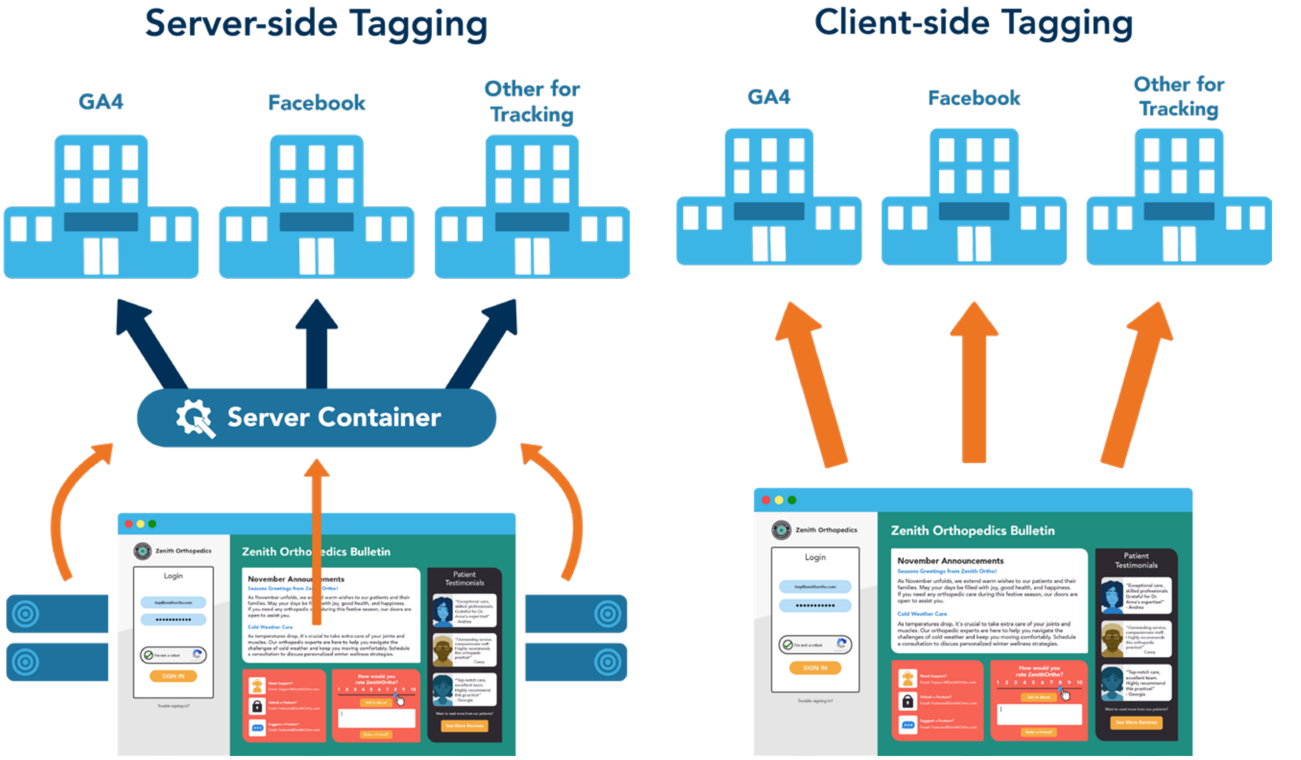
Kentucky ✓

Louisiana ✓

**This data anonymization method described here still has HIPAA compliance implications as it still transfers non-secure data to Google and temporarily stores non-anonymized data. This method should only be used as a risk reduction method while server-side tagging is being implemented.*

Digital Marketing While Maintaining HIPAA Compliance

- Server-Side Tagging: Server-side tagging is a method that allows you to use Google Analytics 4 and maintain HIPAA compliance. This method requires that you install Google Tag Manager (this is a way to manage tags in GA4) on a separate server, redact information, and then send data to GA4 for processing. Client-side tagging is that one sends data directly to Google from your website. Server-side tagging allows you to store the data in a secure location, anonymize the data, and then send it to Google for processing.



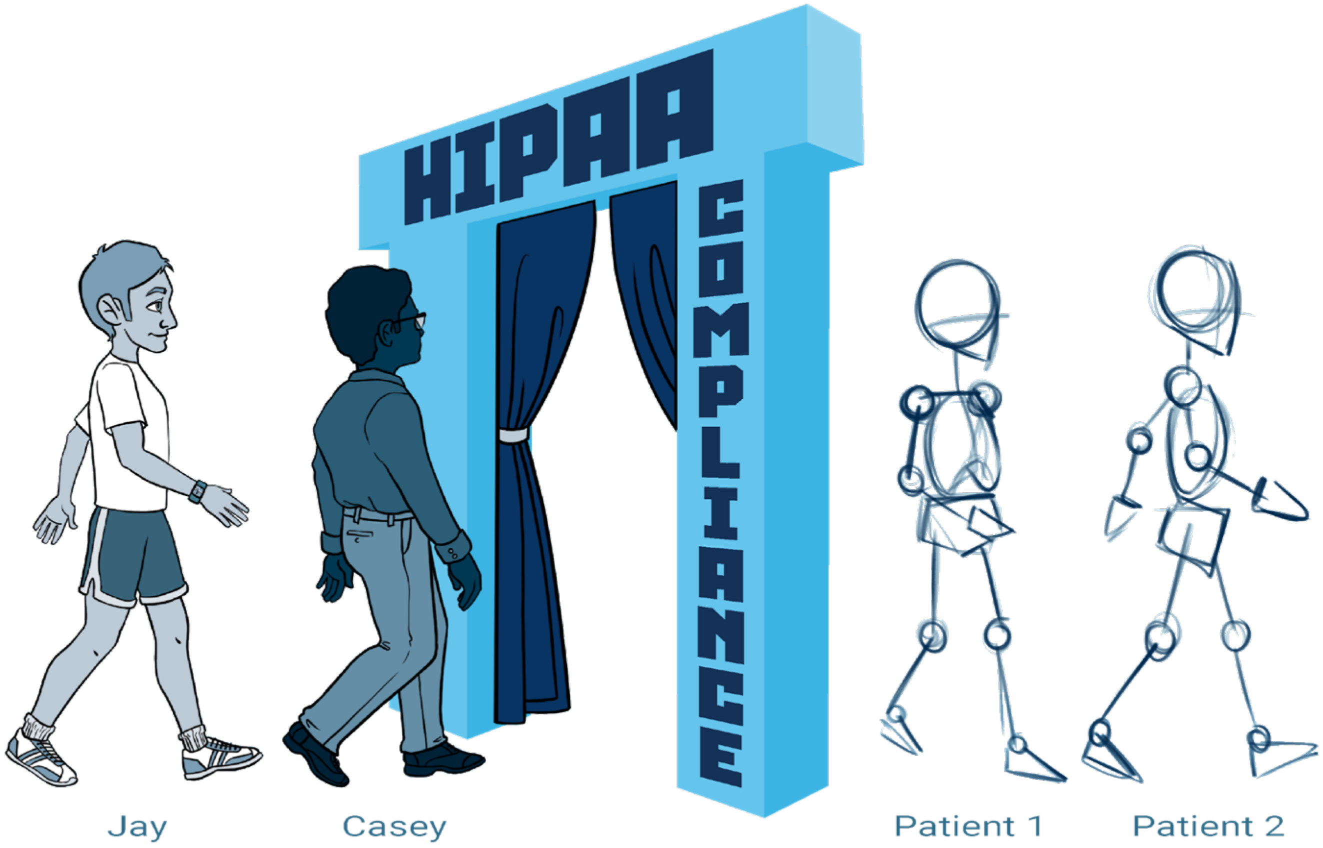
Server-side tagging (pixel placement) gives you control over HTTP requests before sending them to tools for analytic processing. This method will allow you to obfuscate data like IP addresses or healthcare specific pages so PHI or HIPAA protected data is not transferred or even stored temporarily with Google. More information about Server-Side tagging can be found below.

[Why and When to use Server-Side Tagging]

[Configuring and Setting up Server-Side GA4]

Need help? SocialClimb will assess your online HIPAA-compliance.
Contact your CSM or visit us at marketing.socialclimb.com/hipaa-compliance

Digital Marketing While Maintaining HIPAA Compliance



- **Use HIPAA-Compliant Tools:** Use tracking tools and platforms that are designed to be HIPAA-compliant or can be configured to meet HIPAA standards. Ensure that third-party providers have signed a BAA and have appropriate data protection measures and certifications in place, such as SOC 2. Vendors that have a current BAA in place will be able to track your marketing efforts in a HIPAA-compliant way.
- **Train Marketing Staff:** Provide training to marketing staff who handle your website, patient portal, or any applications that you may have. Ensure that they are aware of the regulations and the importance of safeguarding patient information and the specifics of how combined data can create PHI.
- **Schedule Regular Audits and Compliance Checks:** Conduct regular audits and compliance checks to ensure that tracking mechanisms and digital marketing efforts align with HIPAA and other relevant regulations.
- **Limit Data Collection:** Collect only the data that is necessary for your marketing efforts and ensure that it does not include sensitive health information.

Maintain WordPress HIPAA Compliance

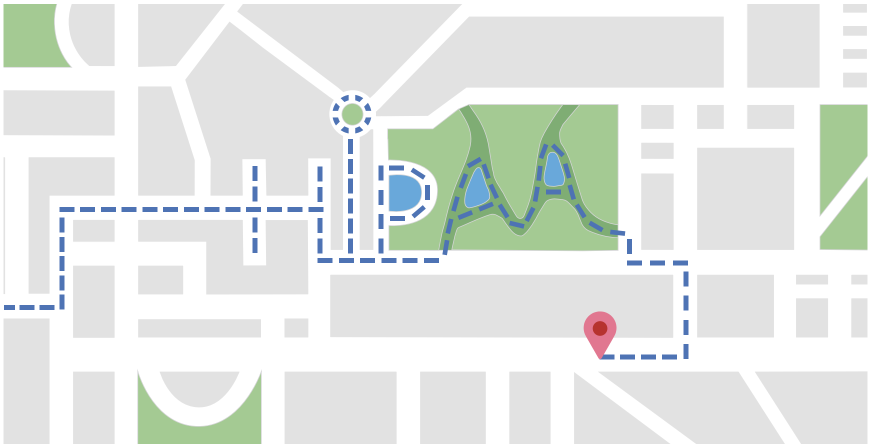
- **Use HIPAA-Compliant Targeting:** Prospective patient targeting products identify nearby individuals who need the healthcare you provide and allow you to target them with specific messaging. Lookalike audiences using public data and CRMs typically have prospective patient data that meets HIPAA requirements.
- **Consult Legal Experts:** Seek legal counsel or consult with experts in healthcare compliance and digital marketing to ensure that your strategies are in line with current regulations.

WordPress HIPAA-Compliance

Mitigating HIPAA compliance issues associated with WordPress and non-compliant plugins involves a systematic approach to ensure the protection of patient health information (PHI).

- **Vet Plugins:** Use WordPress plugins with a focus on security and HIPAA compliance.
- **Update and Maintain:** Update both WordPress and plugins to address vulnerabilities promptly.
- **Implement Strong Access Controls:** Limit PHI access to authorized personnel only.
- Use third-party solutions or custom development to enhance auditing and logging capabilities, creating robust audit trails to track PHI access.
- **Establish Clear Policies:** Train staff to ensure awareness of HIPAA requirements when using WordPress and plugins.
- **Perform Regular Security Assessments:** Complete regular risk assessments to identify and mitigate potential compliance risks proactively.

By combining these measures, healthcare organizations can leverage WordPress while safeguarding PHI and maintaining HIPAA compliance.



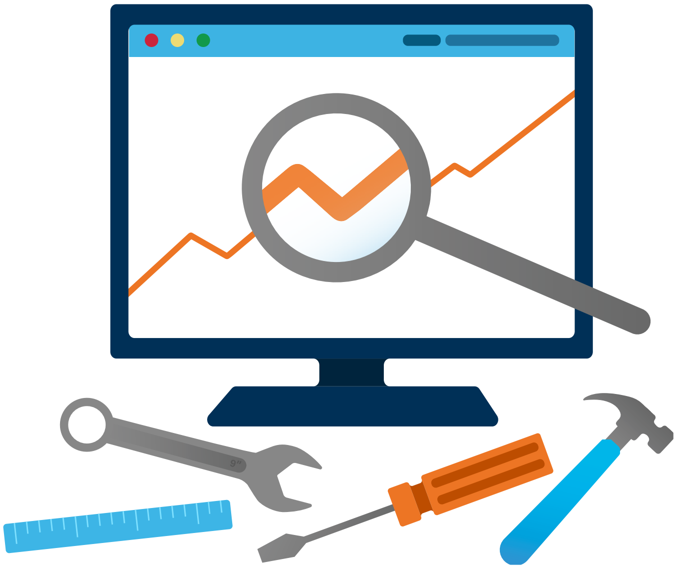
Summary

Summary

By following these guidelines and maintaining a strong focus on patient privacy and HIPAA compliance, you can still track their marketing efforts effectively, protect patient data, and mitigate risks while staying within the bounds of the law.

Marketing in the healthcare industry presents unique challenges due to HIPAA limitations that restrict the collection and use of patient data for targeting outreach. While traditional pixel or script tracking on advertising and social media platforms can be problematic, healthcare providers using SocialClimb use alternative HIPAA-compliant ways to track marketing efficacy. By integrating with PM/EHR software, SocialClimb provides healthcare organizations with HIPAA-compliant tracking tools for in-depth marketing analysis, ensuring patient data security while optimizing marketing strategies.

Contact SocialClimb to Unlock Healthcare Marketing with HIPAA-Compliant Tracking.



Disclaimer

SocialClimb can help assist healthcare organizations in identifying potential HIPAA-compliance risks related to tracking pixels or scripts on their websites and other marketing efforts. While we strive to provide valuable insights and guidance, it is important to note that our assessments and recommendations are based on incomplete information provided at the time of evaluation.

Please be aware that our assessments are not a substitute for legal advice or a comprehensive HIPAA-compliance audit conducted by legal experts. It is essential for healthcare organizations to consult with legal and compliance professionals who specialize in healthcare data privacy and HIPAA regulations to ensure complete and ongoing compliance.

Additionally, the evolving nature of healthcare regulations and digital marketing practices means that compliance requirements may change over time. SocialClimb cannot guarantee that our assessments will cover all possible compliance aspects or guarantee immunity from compliance risks. Healthcare organizations are encouraged to stay updated with the latest HIPAA regulations and seek expert guidance to address specific compliance concerns.

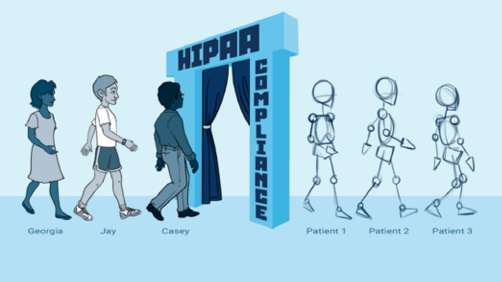
By using SocialClimb's services, you acknowledge and agree that our initial HIPAA assessment is intended to provide general guidance and awareness about potential compliance risks related to tracking pixels or scripts. It is your responsibility to take appropriate actions to address any identified risks and ensure ongoing compliance with HIPAA and other relevant healthcare regulations.

Additional Reading

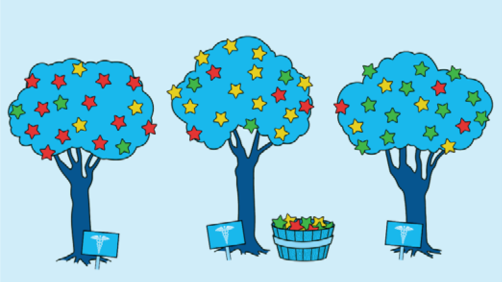
What is a HIPAA BAA and How Does It Affect My Marketing in Healthcare?

Google Analytics Isn't HIPAA Compliant

The Missing Piece of Your Healthcare Marketing Plan: HIPAA-Compliant Call Tracking



HIPAA Compliance in Healthcare Marketing



HIPAA Compliance and Online Review Responses

References

https://compliancy-group.com/hipaa-compliance-quotes/

https://www.aha.org/press-releases/2023-11-02-hospital-associations-and-hospitals-file-lawsuit-challenging-federal-rule-ties-providers-hands-their

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

https://socialclimb.com/blog/what-is-a-hipaa-baa-and-how-does-it-affect-my-marketing-in-healthcare/

https://socialclimb.com/blog/google-analytics-isnt-hipaa-compliant/

https://socialclimb.com/blog/healthcare-hipaa-compliant-campaign-tracking/

https://socialclimb.com/blog/hipaa-compliance-in-healthcare-marketing/

https://socialclimb.com/blog/hipaa-compliance-and-online-review-responses/

https://marketing.socialclimb.com/hipaa-compliance

https://developers.google.com/tag-platform/learn/sst-fundamentals/3-why-and-when-sst?continue=https%3A%2F%2Fdevelopers.google.com%2Ftag-platform%2Flearn%2Fsst-fundamentals%23article-https%3A%2F%2Fdevelopers.google.com%2Ftag-platform%2Flearn%2Fsst-fundamentals%2F3-why-and-when-sst

https://developers.google.com/tag-platform/learn/sst-fundamentals/5-sst-setup-analytics?continue=https%3A%2F%2Fdevelopers.google.com%2Ftag-platform%2Flearn%2Fsst-fundamentals%23article-https%3A%2F%2Fdevelopers.google.com%2Ftag-platform%2Flearn%2Fsst-fundamentals%2F5-sst-setup-analytics