PRIVACY FIRST

Marketing Technologies
that Prioritize HIPAA Compliance

cardinal

Marketing in a HIPAA World

Marketing in healthcare isn't quite as straightforward as it can be in other industries. After all, HIPAA compliance is front and center, and it has gone through a number of significant changes in the last year.

Now more than ever, healthcare marketers need to walk a fine line between doing what's needed in terms of marketing and adhering to highly important privacy rules.

Since the release of an *HHS bulletin in December of 2022 and FTC complaints* against prominent providers, that line has become even finer.

THE GOOD NEWS?

01

Marketing in a HIPAA world is still doable with the right tools in place. To help you, we've put together a list of marketing technologies that *can* be used in a HIPAA-compliant manner.

02

However, it is important to recognize that these technologies often require additional configuration, and may not be compliant directly out of the box.

What is PII & PHI?
When Can a HIPAA Violation Occur?

A HIPAA violations occur when you **combine** personal identifying information (PII) with protected health information (PHI), both explicit and implied.

PII + **PHI**

Examples of PII:

Name
IP Address
Phone Number
Email Address
Device ID
Medical Record Number

Implied PHI:

A visit to a specific condition page

Explicit PHI:

Website form submission that contains health information

Let's walk through an example.

A user visits your website, providing you with an IP address or device ID. While on your site, that user visits a specific page (**oncology treatment)** and you use that information to infer that the user *has* that healthcare condition, then market to them accordingly (**using their device ID**).

That is what would constitute a HIPAA violation under these new guidelines.

BAAs

A crucial piece of this new puzzle for healthcare marketers is the BAA or Business Associate Agreement. A business associate agreement defines a legal relationship between HIPAA-covered entities, such as doctors and practices, and business associates (i.e., tech tools, software, etc.) that can potentially access PHI during the course of their work for a HIPAA-covered entity. This type of agreement is designed to ensure complete protection of a patient's PHI.

How do they make technology and apps HIPAA compliant? Well, a BAA alone doesn't make a technology HIPAA compliant—it's one component of a broader compliance strategy. Technology providers must also implement technical, administrative, and physical safeguards, including but not limited to data encryption, access controls, and audit controls.

It's important to know that getting a BAA in place is not always easy, either. Some marketing technologies and ad platforms will not sign them (E.g., Facebook and Google Ads). Moreover, even if a technology vendor is willing to sign, they may insist on their own agreement, rejecting your organization's BAA. This often becomes a contentious issue for compliance teams, and reaching a compromise can become elusive.

While exploring HIPAA-compliant marketing tools, remember to independently investigate each technology. Signing a BAA is not a universal solution; evaluate their agreement, terms of service, and data management processes diligently.

Customer Database Platforms (CDPs)

What do you do when a marketing technology vendor won't sign a BAA? In the instances where you need to use the tool, you can consider implementing a CDP or Customer Database Platform.

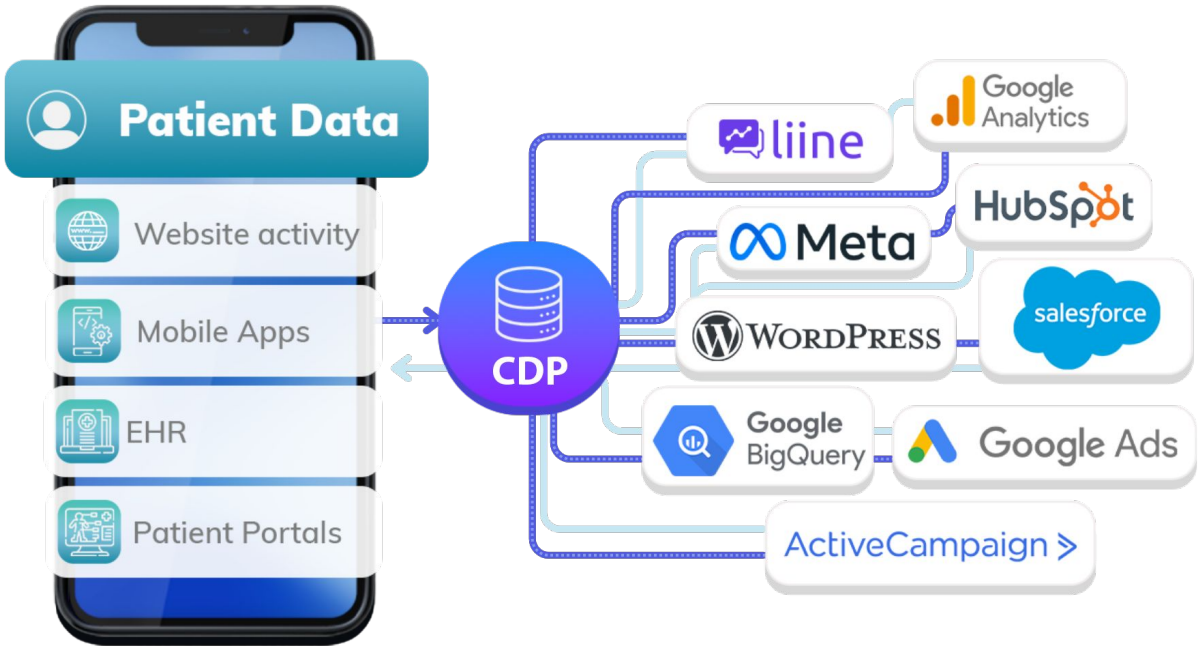
WHAT IS A CDP

CDPs are technologies that can help you protect patient health information and ensure the anonymity of your website users. They achieves this through several mechanisms.

1. **CDPs employ robust data encryption techniques to secure patient information during transmission and storage. This encryption ensures that the data remains protected even if it is intercepted or accessed by unauthorized individuals.**
2. **CDPs often implement strict access controls, limiting data access to authorized personnel who require it for legitimate purposes. This prevents unauthorized individuals from viewing or manipulating patient health information.**

How CDPs Work

CDPs are built to be flexible and interoperable, allowing seamless integration with your existing systems, applications, and marketing technologies.



Anonymization Techniques:
The CDP applies anonymization methods to PHI, transforming it into non-identifiable and de-identified data. This may involve techniques such as removing direct identifiers (e.g., names, addresses) or using cryptographic hashing to replace identifying information with irreversible pseudonyms.

Data Segregation:
The CDP creates distinct data silos or partitions to isolate PHI from other types of customer and marketing data.

Preserve Your Existing Tech Stack w/ CDPs

By anonymizing the data, CDPs help ensure that patient health information is stripped of identifying details, making it nearly impossible to link the data back to specific individuals.

These measures collectively safeguard patient privacy, protect health information, and allow marketers to use other technologies in a HIPAA-compliant manner. With identifying information removed, marketers, for example, can pass information between data sources like Google Analytics and Google Ads.

Rest assured, if you wish to retain your current technology stack and reporting solutions, implementing a CDP offers the simplest and most seamless solution. Once the CDP is successfully implemented, you can continue using your existing tools, processes, and dashboards.

CDP Options

Which CDPs should you consider? Here are a few options:

- ***Freshpaint*** **offers a HIPAA mode to achieve compliance.**
- ***Rudderstack*** **offers HIPAA compliance with its Enterprise custom pricing.**
- ***Segment*** **is able to sign BAAs for managing PHI, or PII that should be treated as PHI.**

Not Every Tool Needs to Be HIPAA-Compliant

Just because a technology isn't HIPAA compliant doesn't mean it's off-limits to you as a healthcare marketer.

Remember, not every marketing tool captures PHI. To ensure that your solution is not capturing PHI, it's important to understand what PHI is in the eyes of the HHS and how you're using data.

According to the HHS, PHI is «individually identifiable health information», including demographic data, that relates to:

- **the individual's past, present, or future physical or mental health or condition**
- **the provision of health care to the individual, or**
- **the past, present, or future payment for the provision of health care to the individual**
- **and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).**

When implementing new technologies, ensure you fully understand how the tech will be used, what information is being captured, and where (and how) it's being stored and sent. Train your marketing and operational team to understand data management best practices.

As an example, you never want anyone on your team thinking it's okay to upload customer lists to an ad platform like Facebook or an email marketing platform that hasn't signed a BAA!

PAY ATTENTION

You will need to be especially vigilant with staff that come from other industries, such as retail or eCommerce. They've been using marketing tech and customer data differently and may need special training to ensure that they understand how different the stakes are in healthcare.

HIPAA-Compliant Solutions by MarTech Category

With all of this in mind, what are the HIPAA-compliant solutions you can use as a healthcare marketer? Let's walk through the most relevant technologies that most marketers use and explore the solutions that comply with HIPAA due to their data management processes and willingness to sign a BAA.

- **Call Tracking & Analytics Solutions**
- **Website CMS & Add-ons**
  - Website Forms
  - Online Schedulers
  - Chatbots & Live Chat Solutions
- **SMS Marketing Platforms**
- **Reputation Management Tools**
- **Marketing Automation & Email**
- **Customer Relationship Platforms (CRMs)**

HIPAA-Compliant Call Tracking & Analytics Solutions

Call tracking and analytics is a vital technology in the healthcare marketing toolkit. It provides insights into where your leads are coming from, what they want, and if they ultimately book an appointment.

The most innovative of today's call-tracking solutions leverage AI to track and analyze phone calls and identify crucial data points, including patient sentiment, conversion barriers, lead quality, and more. With this data in hand, marketers can then identify which campaigns, keywords, and resources are generating calls and form fills, enabling them to allocate spend and optimize strategy more effectively.

CHECK OUT

While there are a number of options out there, we here at Cardinal see our clients use these call-tracking solutions:

liine

PATIENT PRISM

CallBox

Other options to consider?

INVOCA

CallRail

Marketing Analytics & Data Visualization

GOOGLE ANALYTICS

The go-to analytics solution for many marketing teams has long been Google Analytics. While a hugely popular and effective tool, it is *not inherently HIPAA-compliant*. Google places the onus directly on marketers, stating that users should not pass any data to Google "that Google could recognize as personally identifiable information (PII)" or that could be considered PHI.

Here's why it's so difficult for Google Analytics to remain compliant: Say a man in the Cincinnati area is looking for mental health treatment for a particular condition. After googling "treatment for [condition] Cincinnati," that potential patient clicks on a link to your site on the search results page.

Google Analytics' tracking tool will collect your page URL along with the IP address of the potential patient. As we illustrated earlier, these two pieces of information put together violate HIPAA regulations because a connection has been made between a piece of PII (the patient's IP address) and your URL—potentially identifying the patient's condition.

While a Customer Data Platform (CDP) can be used to make Google Analytics compliant, you can also use other analytics tools.

ALTERNATIVES

When it comes to analytics solutions, the tools shown below will sign a BAA and offer a solid alternative to Google Analytics 4:

mixpanel Heap Amplitude

Secure & Compliant Website Technologies

Websites remain an essential first point of contact for patients, serving as the foundation of most patient acquisition strategies. For many, research into a condition and/or care starts online, and websites can serve as a way to continue research, evaluate providers, and, of course, schedule initial appointments. On the provider side, websites can include important tools for communicating directly with potential patients, including chatbots, forms, and live chat.

CHECK

Now more than ever, however, healthcare marketers need to ensure that they are using secure and HIPAA-compliant tools with their websites.

Website CMS

Chances are, if your site is doing its job, it will be "handling" PHI at some point. Whether patients are filling in forms, engaging in live chats, or just viewing condition web pages, there's the opportunity to transmit PHI. For this reason, whatever content management system (CMS) you use must be HIPAA-compliant or offer integrations and plugins to meet security and privacy requirements.

Here are common CMS, along with some details on how they address compliance:

WordPress

Making a WordPress site *HIPAA-compliant* is possible with the right tools and data management strategies. It involves implementing security controls and protocols that meet the requirements defined by the HHS. The *HIPAA Journal* recommends that you:

- **Host the website on a *HIPAA-compliant host* or with a hosting company willing to sign a BAA.**
- **Ensure that any data uploaded to the website (via form) is through a HIPAA-covered plugin (more ahead).**
- **Use security plugins like *WordFence* to conduct routine security scans and log CMS user access records.**
- **Implement two-factor authentication for all website administrators and users.**
- **Train all website users on privacy and security best practices.**
- **Store electronic PHI separately from WordPress and ensure data encryption during transit and at rest.**

Joomla!

Like WordPress, Joomla has a two-factor authentication plug-in available that can be used to protect HIPAA-controlled data and keep it secure.

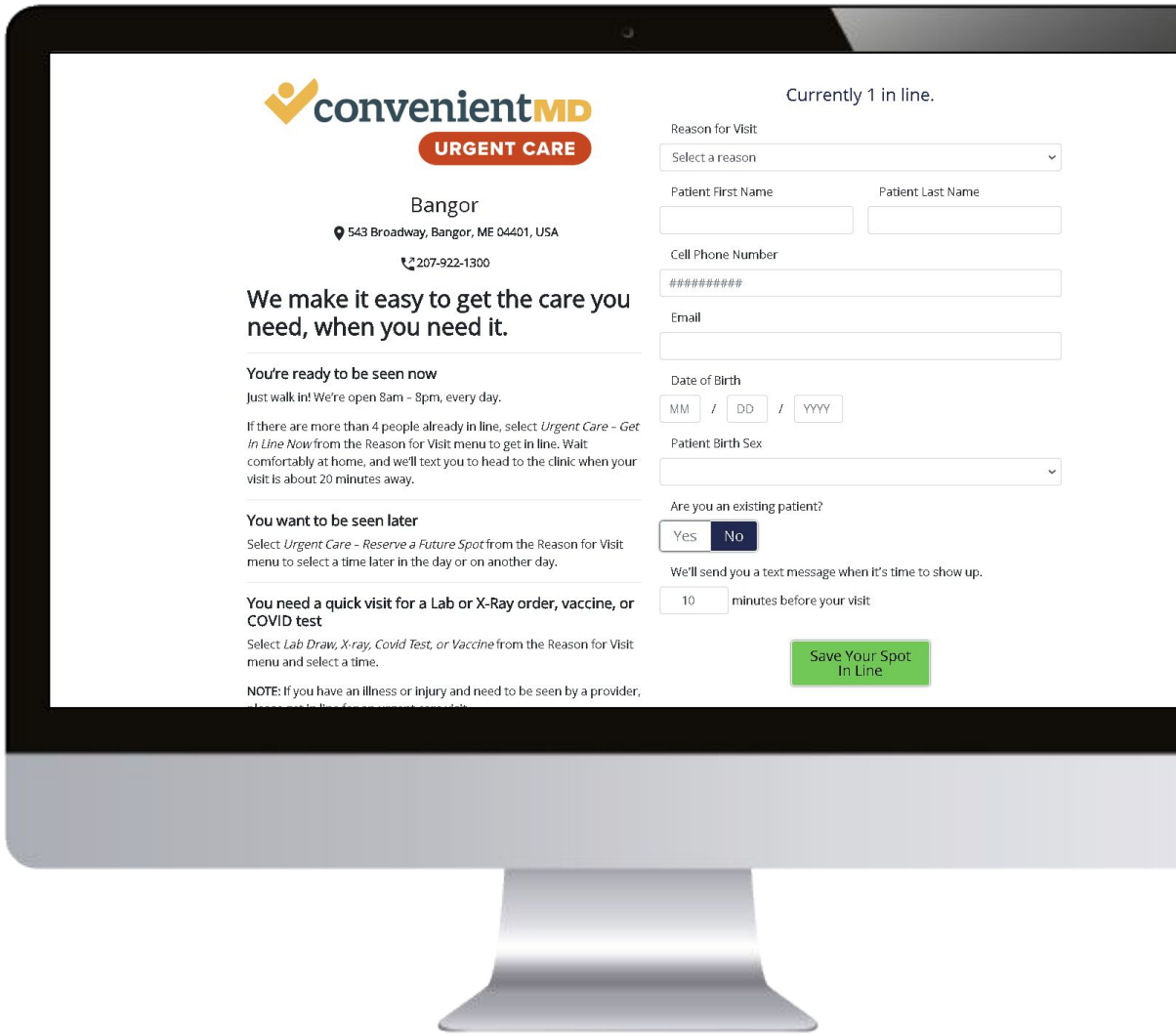
Drupal

Things get a bit more complicated with Drupal, as it's a platform that requires more sophisticated developers and customization. It can get the job done and achieve HIPAA compliance with add-ons.

Website Forms

Patients today want to take action on websites, and one of the main ways they do that is by filling in forms to book appointments. Often, healthcare groups will use these forms to collect PHI, raising the stakes when it comes to compliance. An open text field in a form asking “why are you contacting us” allows a user to enter PHI and exposes you to risk.

As a precaution, we recommend limiting the information you’re collecting. Instead, direct people to a HIPAA-compliant online booking platform whenever possible.



TOP OPTIONS

If you do use forms, check out the following solutions:

FormDr — Built for multi-location practices and offers the ability to direct form submissions to appropriate intake locations or providers.

formstack — Offers mobile-friendly, HIPAA-compliant forms that include data encryption, user-level permissions, audit logging, and security maintenance.

logiforms — HIPAA and PCI-certified form solutions include SSL, RSA encryption, and two-factor authentication.

MedForward — Submissions are encrypted in transit and at rest and are served over a protected SSL certificate.

GRAVITY FORMS DOCS — You will need to use the HIPAA FORMS plugin to ensure that you are HIPAA-compliant.

Jotform — HIPAA-compliant forms are only available with JotForm's Gold plan.

FormAssembly — HIPAA-compliant forms are only available with Enterprise and Government plans.

Chatbots & Live Chat

Patients have questions, and they want them answered as soon as possible. That's where chatbots and live chat come in, providing healthcare groups and marketers with a way to engage patients when they want help.

What are the best options when it comes to these site tools? Take a look at *Smartbot360* as your chatbot solution; it's built specifically for healthcare.

If you want live chat grouped with a chatbot solution, consider the following:

LiveChat

HIPAA compliance is only available with an Enterprise account.

freshworks

HIPAA compliance is only available with the standalone version of Freshchat.

TeamSupport

HIPAA compliance is only available through an add-on.

Online Schedulers

Today's patients want the option of scheduling online; for that reason, many healthcare groups and their marketers turn to online schedulers, which allow patients to initiate the process themselves online. Looking for information is one thing—scheduling an appointment is another that can often capture PHI.

NextPatient

nexhealth

DaySmart Appointments

10 to 8 Powering appointments, for time better spent.

CareCloud

ACUITY SCHEDULING

Advertising Integration

NexHealth passes data back to Google Ads so you can track campaign performance and train the algorithm on the leads that converted into booked appointments. So not only are you giving patients a seamless booking experience, you're gaining valuable insights to improve your campaign performance (all in a HIPAA-compliant manner).

SMS Marketing Platform

Patient no-shows and dropouts are always a concern in healthcare. SMS marketing and communication tools give practices and marketers an easy way to maintain contact with patients and remind patients of upcoming or follow-up appointments.

TOP OPTIONS

qliqSOFT

Notifyd

tigerconnect

Reputation Management Tools

As patients research, they often look into a practice's reputation online. Reputation management tools can help you stay on top of your online reputation by automating review solicitation, compiling reviews in one place, and allowing you to respond when not-so-great reviews come in.

Marketing Automation & Email Marketing

Ideally, patients and practices have ongoing, long-term relationships. One of the most effective ways to manage patient relationships in the long term is to leverage marketing automation and email marketing tools. You can use these solutions to keep patients up to speed on new services, share promotions, and engage patients between appointments.

HubSpot, a widely used marketing automation software platform, is not HIPAA compliant due to its terms of service, which explicitly prohibit users from collecting, storing, and transmitting sensitive health information. Despite this limitation, healthcare marketers can still use HubSpot by implementing effective data management strategies and third-party tools to prevent the platform from being exposed to PHI.

HIPAA Compliant CRMs

Our clients in the healthcare space use these CRMs:

CRMs or customer relationship management solutions serve as a database of patient actions and choices, giving you the information you need to improve patient outcomes and increased patient satisfaction.

ZOHO

enquire®

mend

salesforce

Requires security customizations and add-ons to become HIPAA compliant

freshworks

Requires a signed BAA to become HIPAA compliant

cardinal
digital marketing

Take Flight

with Cardinal Digital Marketing

Reach out with your HIPAA questions:

Alex Membrillo
CEO, Cardinal Digital Marketing
am@cardinaldigitalmarketing.com

Or visit us at:

www.cardinaldigitalmarketing.com

Legal Disclaimer: Marketing Technology Vendor List

The following disclaimer outlines the purpose and limitations of listing the marketing technology vendor within this guide. Please carefully read this disclaimer before utilizing the information:

Informational Purpose: The technology vendor recommendations are intended solely for informational purposes. They are not intended to serve as legal advice or replace the expertise of legal professionals. The recommendations are based on general industry knowledge and best practices available at the time of compilation.

No Attorney-Client Relationship: The vendor recommendations do not establish an attorney-client relationship between Cardinal Digital Marketing and the user. The information provided does not create any legal obligations or privileges.

Independent Investigation: Users of the vendor list should conduct their own independent investigation and research to evaluate the suitability of marketing technology tools for their specific needs and to ensure compliance with relevant legal and regulatory requirements, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) regulations.

Individual Circumstances: The vendor recommendations may not be applicable to all situations, as individual circumstances and legal requirements can vary. It is essential for marketers to consult their own legal and compliance teams to assess their unique circumstances and determine the most appropriate marketing technology tools to implement.

Compliance with Laws and Regulations: Implementing marketing technology tools, particularly those related to HIPAA compliance, may require adherence to specific legal and regulatory requirements. The vendors compiled in this guide legal advice and should not be solely relied upon to ensure compliance. Users are strongly encouraged to consult legal and compliance professionals to address their specific obligations.

Limitation of Liability: Cardinal Digital Marketing, its employees, affiliates, and agents shall not be held liable for any direct, indirect, incidental, consequential, or special damages arising out of or in connection with the use of the vendor recommendations or reliance on the information provided, even if advised of the possibility of such damages.

Third-Party Content: The vendor recommendations may contain references or links to third-party websites, tools, or resources for informational purposes. Cardinal Digital Marketing does not endorse, control, or take responsibility for the accuracy, content, or availability of such external resources.

Updated Information: The vendor recommendations provided by Cardinal Digital Marketing may not reflect the most current legal developments or requirements. While efforts are made to provide accurate and up-to-date information, it is essential for users to independently verify the latest legal obligations and compliance standards.

Legal Consultation: Cardinal Digital Marketing strongly advises marketers to consult their legal and compliance teams before making any decisions or implementing new technologies. Qualified legal professionals are best positioned to assess the specific legal implications, provide advice on compliance requirements, and help mitigate potential risks associated with marketing technology implementation.

By utilizing the vendor recommendations listed in this guide, you acknowledge that you have read, understood, and agreed to the terms of this legal disclaimer. You further understand that the vendor recommendations are not a substitute for seeking legal advice from qualified professionals and that Cardinal Digital Marketing shall not be held responsible for any consequences arising from your reliance on the information provided.

If you do not agree with the terms of this disclaimer, it is advised that you refrain from using the vendor recommendations provided in this guide.