CallRail

A resource guide book for

HIPAA and HITECH requirements for covered entities using call tracking software

Introduction

Like most businesses, many medical practitioners market themselves to potential new customers and patients. Call tracking provides key insights into which of these marketing channels and online ads provide the highest-quality leads. However, maintaining the privacy and security of protected health information can introduce significant challenges to out-of-the-box call tracking solutions.

From scheduling appointments to billing, referrals, and prescription refills, private information can be communicated over the phone between patients and their healthcare provider. This information is protected under the Health Insurance Portability and Accountability Act (HIPAA) and its expansion, Health Information Technology for Economic and Clinical Health Act (HITECH). If you're a healthcare provider or marketing agency that services one, you need to ensure you are following HIPAA requirements and keeping data secure.

CallRail's healthcare plans help covered entities and the marketing agencies serving them continue to meet the requirements set forth by HIPAA and HITECH.

In this quick guide for HIPAA compliance and call tracking, you'll learn:

Chapter 1
The history between HIPAA compliance and call tracking

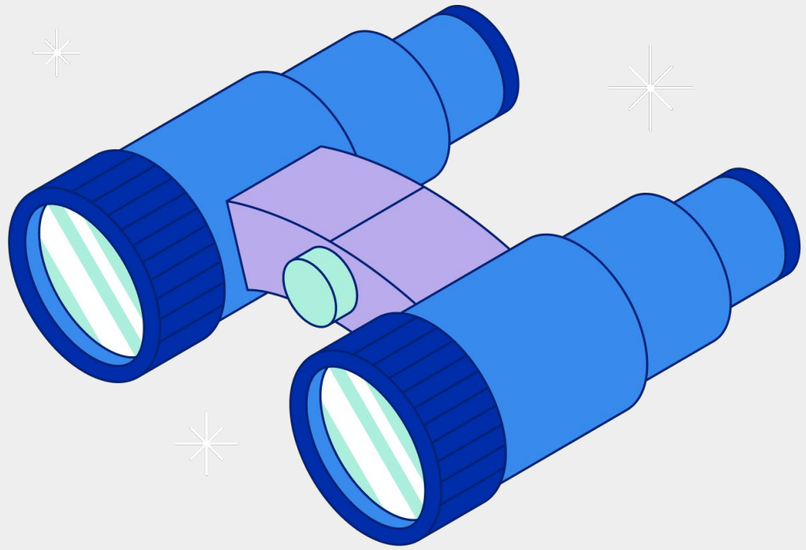
Chapter 2
Why following HIPAA Guidelines in call tracking is a priority

Chapter 3
Who can help you comply with HIPAA requirements for call tracking

Chapter 4
Why do businesses need HIPAA-compliant call tracking

Chapter 5
CallRail's HIPAA implementation and data security measures

Chapter 6
Three helpful compliance tips



Chapter 1

HIPAA compliance and call tracking: *A history.*

HIPAA, originally known as the Kennedy-Kassebaum Bill, is a set of regulations that became law in 1996. These laws help people carry their health insurance and medical records from one healthcare institution to the next. In addition, HIPAA has also created a system to recognize and enforce the rights of patients to protect the privacy of their medical records.

But what does that have to do with call tracking?

In 2009, HIPAA was expanded by the Health Information Technology for Economic and Clinical Health Act (HITECH) to cover all businesses associated with access to health information, which includes call tracking providers.

The law now requires that all patient health information be protected from disclosure and misuse by the practitioner and any business associates that have access to that information, such as CallRail.

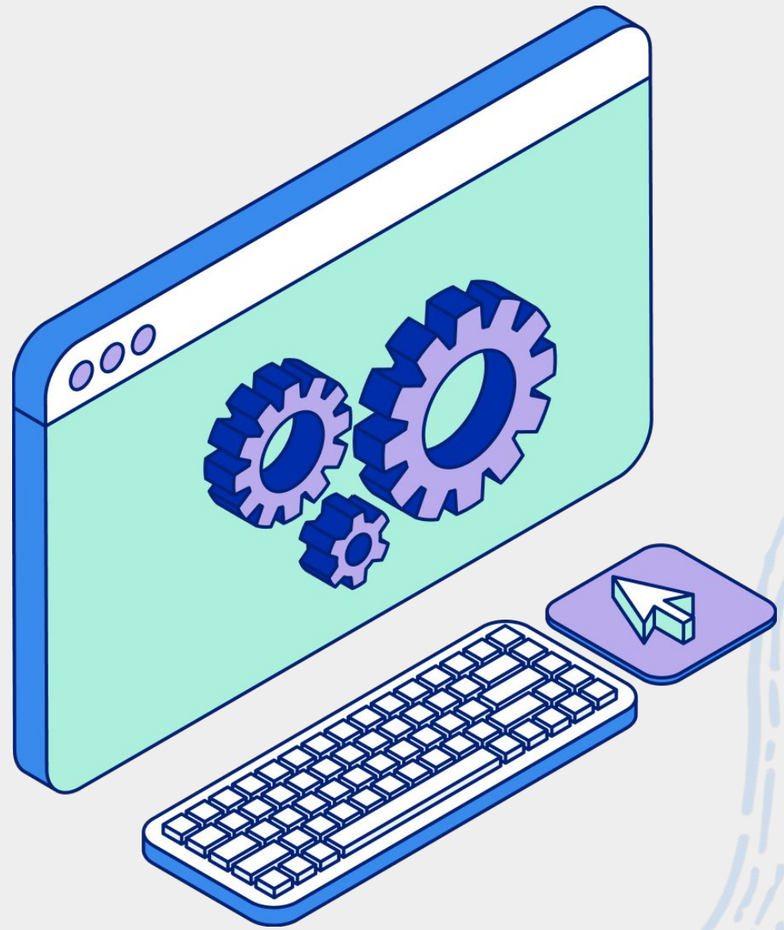
This personal health information is known as Protected Health Information (PHI), according to HIPAA.

How does the December 2022 bulletin from the Office for Civil Rights (OCR) impact call tracking in healthcare?

In December 2022, the Office for Civil Rights (OCR) released a bulletin outlining concerns regarding healthcare and call tracking. (1)

The good news? In the bulletin, the OCR stated that the collection and processing of PHI via online tracking is permissible to assist with the running of healthcare operations. HIPAA regulations require that PHI is not shared with third parties, unless an appropriate Business Associate Agreement (BAA) is in place or patient authorizations have been obtained. (2)

CallRail takes HIPAA compliance seriously; that's why we've created an end-to-end solution for healthcare providers and sign a Business Associate Agreement (BAA) with each of our covered entities. This collaborative effort ensures that covered entities and the agencies supporting them maintain compliance with HIPAA and HITECH regulations. Additionally, CallRail continues to maintain our series of essential security and privacy safeguards to assist our clients with compliance.



Chapter 2

Why following HIPAA Guidelines in call tracking is a priority

Two different types of PHI are stored in CallRail:

1. **Call recordings** - may contain personal information and medical history
2. **Caller ID information** - Phone number of caller, Caller ID Name (CNAM) and potential specific marketing campaign identifiers

Phone calls are personal, one-on-one conversations between health providers and the patients and customers they serve. They may involve the discussion of private issues and medical history. While recording incoming calls can provide significant benefits in determining lead quality and training staff members, the contents of these conversations can contain personal health information. Consent for call recordings is the responsibility of healthcare businesses to provide to their patients.

Even without an audio recording of the call, the fact that the call happened at all may create health information that links an individual to a medical practice and the types of services they provide. If the call is to a tracking number that indicates a specific marketing campaign, or one that links an online visitor and their search keywords, an even greater picture of the caller's medical needs and history begins to emerge.

WHAT THE LAW REQUIRES

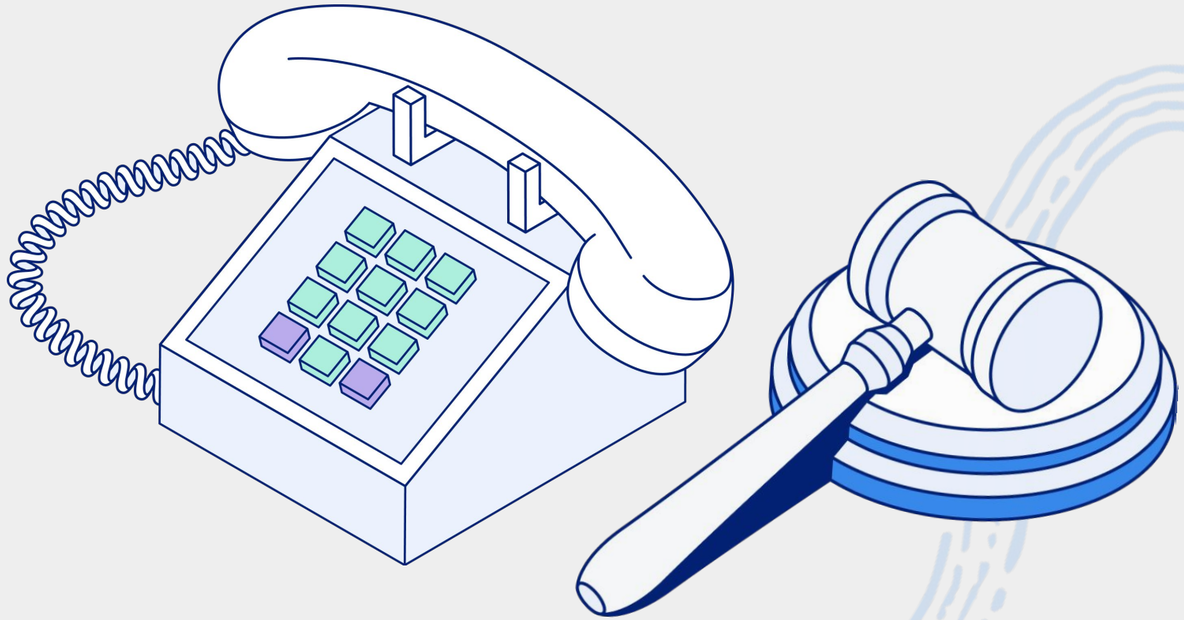
There are two key components to HIPAA compliance: the Privacy Rule, and the Security Rule.

The Privacy Rule

The Privacy Rule dictates what is considered Protected Health Information (PHI), and who may use and access this information.

According to the Privacy Rule, use of call tracking falls under the administrative operations usage of PHI. It is acceptable for this PHI to be shared with CallRail, but only when a Business Associate Agreement (BAA) is in place. If a marketing agency is assisting the healthcare provider then two cascading BAAs are recommended —one between the provider and the marketing agency, and one between the marketing agency and CallRail.

Optionally, when a provider uses an agency, the provider may enter into a BAA directly with CallRail.



The Security Rule

The Security Rule describes how this information is protected, including operational safeguards and technical measures.

The Security Rule requires CallRail to have operational safeguards in place to prevent unauthorized disclosure of PHI. CallRail has these measures in place, but the BAA is legally required to guarantee this to the healthcare provider for proper compliance with HIPAA regulations. In addition, the Security Rule requires additional technical safeguards, which are enabled for CallRail's Healthcare customers.

Chapter 3

Who can help you comply with HIPAA requirements for call tracking?

Covered entities must select a provider that takes their HIPAA compliance responsibility as seriously as they do. It is crucial to work only with service providers who have designed an end-to-end solution to meet the requirements of HIPAA and HITECH. Those providers will be willing to sign a Business Associate Agreement certifying their implementation and responsibilities.

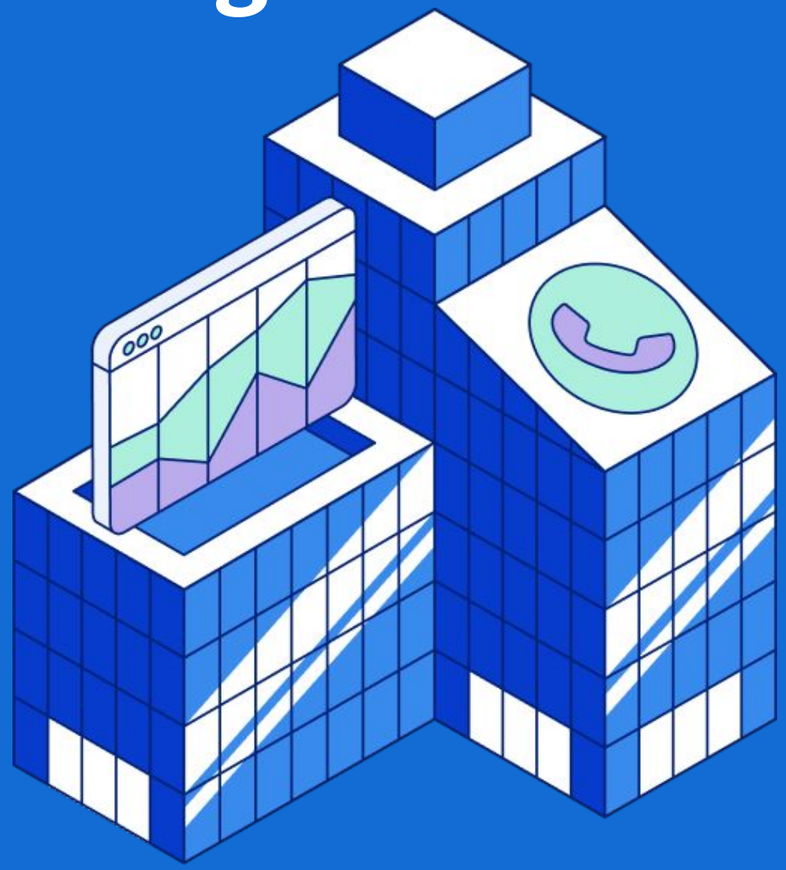
At CallRail, we take HIPAA compliance seriously. That's why we've not only created an end-to-end solution for healthcare providers, but we also sign a Business Associate Agreement (BAA) with each of our covered entities on our healthcare plans.

Entering into a Business Associate Agreement allows delegation of specific operational responsibilities to third-party service providers such as CallRail. This BAA grants the third-party service provider the right to collect and store Protected Health Information on behalf of the healthcare provider.

CallRail's software, platform, infrastructure, and processes have all been carefully designed to ensure that clients' data is protected and their responsibilities fulfilled.

Chapter 4

Why do businesses need HIPAA-compliant call tracking?



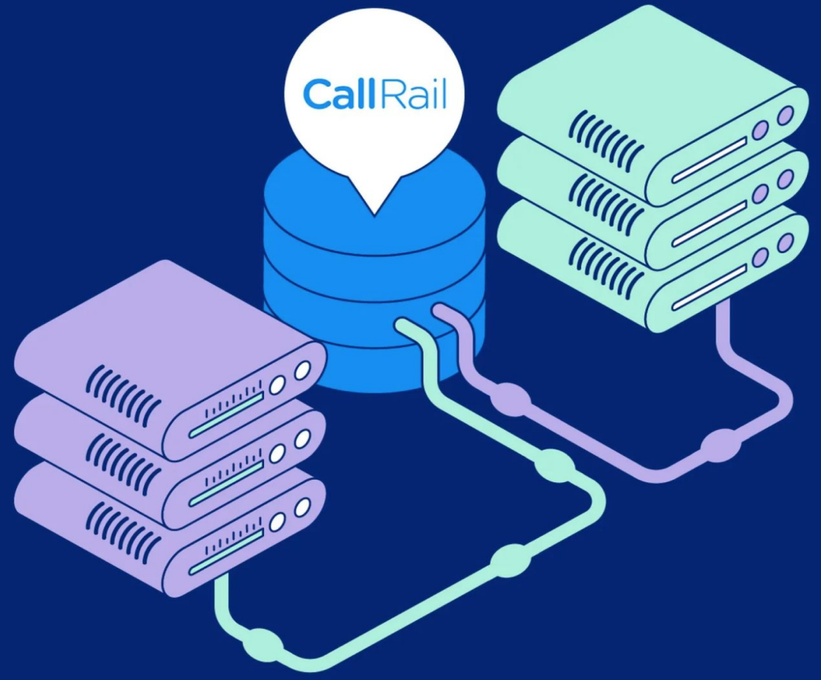
Not only are healthcare businesses legally obligated to follow privacy rules, but client and patient retention is also correlated to knowing private medical information is secure. Plus, there are huge fines and even jail time associated with HIPAA/HITECH violations.

Note, that HIPAA protections apply to current and prospective patients, so it is essential that all marketing tools and 3rd-parties are HIPAA compliant.

As of October 2023, the Office for Civil Rights (OCR) has received over 342,032 HIPAA complaints. To date, OCR settled or imposed a civil money penalty resulting in a total dollar amount of $136,918,772. (1) In 2022, 55% of the financial penalties imposed by OCR were on small medical practices. (2) Don't be caught without following HIPAA requirements!

Chapter 5

CallRail's HIPAA implementation and data security measures.



CallRail takes data security very seriously for all customers. The following protections are in place for customers on CallRail healthcare plans.

All data encrypted "in transit"

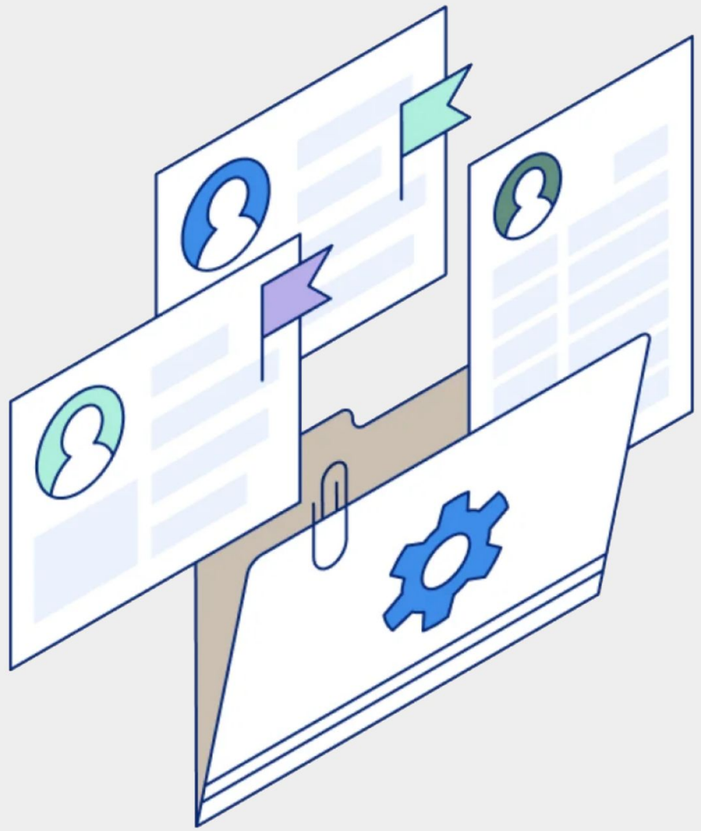
As required by the Security Rule, all access to CallRail is encrypted via SSL to protect data from interception on network points between the user and CallRail. Links between CallRail and other providers are also fully encrypted. Transmission via cipher suites or SSL versions with known weaknesses is prevented.

All data encrypted "at rest"

As required by the Security Rule, all call records, web visitor sessions, and call routing details are fully encrypted when stored on disk. This data is seamlessly decrypted as-needed for reporting purposes when accessed by the customer. Recorded audio is also securely encrypted, and only decrypted when needed for playback and registered to an authorized user. These precautions protect the data even if hard drives fail, or are decommissioned or stolen.

Protection for external systems

Call alert emails, integrations, and other CallRail features could potentially expose PHI to external systems that aren't considered in compliance with HIPAA requirements. In these cases, CallRail prevents transmissions of call details to those systems and instead provides a link that requires the user to log in to review the information. This protection also applies to web visitor sessions, text messages, form captures, and any other data CallRail may collect and record.



Secure access

Individual users are granted their own login credentials, which can be controlled by an administrator. Login sessions automatically expire after a brief period of inactivity to prevent unauthorized access.

Full audit history

HIPAA requires logging for all access and modifications to PHI. For HIPAA plans, all access to the application is logged by user, timestamp, and IP address. Playback of any call recording, as well as all changes to calls, tags, or configuration are similarly logged.

Dedicated, single-tenant equipment

HIPAA requires that the data owner have “hands on” access to all equipment used for data processing. CallRail uses only dedicated hardware and does not make use of virtual machines on shared-tenancy hardware for customers covered by BAA.

Firewalls and private network gap for all machines containing PHI

The databases, application servers, and other machines responsible for routing calls and running the CallRail application and services are isolated and inaccessible via the public internet (except the web application itself, of course). This private network is protected by a pair of redundant hardware firewalls to ensure only expected traffic is allowed.

Included PII/PHI redaction

Included in all of our healthcare plans, we offer free PII/PHI redaction, an extra step in protecting your client and customer data. You need to turn on this feature, but it is included for free with CallRail, unlike with some other call tracking features.

For more information about PII/PHI redaction visit: https://support.callrail.com/hc/en-us/articles/5711436950797-PII-redaction-

Chapter 6

Three helpful compliance tips

While the precautions CallRail has taken can reduce your risk of HIPAA violations, there is still residual risk that can be overlooked.

Where you use HIPAA-compliant call tracking to understand where your best leads come from or to take advantage of call recording for lead qualification purposes, it's important to understand where a tool like CallRail has you protected, but also what additional precautions are needed on your end.

COMPLIANCE TIP #1

Check compliance with all integrations

Whenever you enable a call tracking integration, you are sharing data, potentially including PHI, with any additional business associate.

Under HIPAA, it is acceptable for PHI to be shared with CallRail so long as a Business Associate Agreement (BAA) is in place (which is required to access all CallRail healthcare accounts). If a marketing agency is assisting a healthcare provider and utilizing CallRail then two cascading BAAs are required—one between the provider and the agency, and one between the marketing agency and CallRail.

These same precautions must be in place with any other third-party providers you are sharing PHI from CallRail with, whether they are one of our pre-built integrations or you're utilizing CallRail's open API.

Never connect CallRail to any third-party software unless you're confident the platform is in compliance with HIPAA requirements. If you're using a CallRail healthcare plan, we'll always issue a warning prior to activating any integrations to ensure you maintain compliance from all sides.

COMPLIANCE TIP #2

Never share user credentials

It seems innocent enough—instead of creating a new user for each and every member of your team that needs access to CallRail, you all decide to share the same email address and password for login purposes. Well what seems innocent at first, can be detrimental to your HIPAA compliance.

HIPAA requires logging for all access and modification to PHI. This is to ensure that in the event of any sort of data breach, the proper authorities have access to any user-level errors that may have led to the compromised data.

All CallRail healthcare accounts log access to the application by user, timestamp, and IP address; playback of any call recordings, as well as all changes made to calls, tags, or configurations, are similarly logged. But if there is only one user being used to access an Account or Company, there is no way for us to create a fully accurate audit log.

Therefore, it is in your best interest to create individual user logins for everyone who needs access to your CallRail account. All CallRail healthcare accounts come with unlimited users, in different tiers of access. For extra security, we also recommend activating two-factor authentication.

COMPLIANCE TIP #3

Export with caution

Similar to integrations, CallRail can only maintain HIPAA compliance so long as your call data resides within your CallRail account. Once you use our export option within either the Call Log or Reports, or download an individual call recording, all PHI is leaving the safe and secure home of your CallRail healthcare account.

Exporting data is okay, and here at CallRail we definitely understand why you would need to do that. It is important, however, to ensure the environment you're exporting the PHI to is both secure and compliant. The included PII/PHI redaction feature for our healthcare plans will assist you in maintaining compliance.

If any exported information is going to be shared with another company or client, it is important you determine whether or not a BAA needs to be in place. If you are going to interact with, track, store, manage, or share any health-related information, be sure that it is stored and transmitted in a way that meets the security and privacy guidelines outlined by HIPAA.

Frequently Asked Questions

What are the differences between a standard CallRail account and a healthcare account?

In a CallRail healthcare account:

- CallRail will enter into a Business Associate Agreement (BAA) with the covered entity or business associate
- Users will be logged out every 30 minutes
- There will be restrictions on integrations that send PHI to third parties
- Voicemail transcriptions will not be available
- Accessing the recording link will require a login. In this case, Notification Only users will need to be promoted to Client Manager or Client Reporting users so that they can log into the account to listen to call recordings
- Caller ID information for the caller won't be included in the Call Notification email, but will be available upon logging into CallRail
- Form submissions alerts received via text message won't include any message from the lead, only the telephone number; however, this information will be available upon logging into CallRail
- Text notification emails won't include the message, only the phone number; however, the message will be available upon logging into CallRail

Are any additional features added for the CallRail healthcare plans?

Two security-related features are added for CallRail's healthcare plans. First, users of HIPAA accounts will have sessions that automatically expire after a short period of inactivity. This helps protect against prying eyes when computers are left unlocked. Second, full audit trail logging is enabled to document all access and modification history.

Will CallRail sign a Business Associate Agreement (BAA) with my business?

Yes, CallRail will provide a BAA to cover the agreements with customers. This BAA can be enacted quickly by electronic signature.

Will CallRail alert me if I am out of compliance with HIPAA requirements?

No, CallRail cannot audit customers to determine if their use of the application is subject to HIPAA regulations. Knowing the regulations that apply to a particular scenario is solely the customer's responsibility.

How does CallRail ensure they are up to date on any compliance changes?

To ensure the security and privacy of its healthcare customer data, CallRail engages a third-party audit firm to test its controls in accordance with the HIPAA Privacy and Security rule. CallRail's HIPAA attestation serves as proof that it is fulfilling its obligations and commitments.

Are any features unavailable in the CallRail healthcare plans?

It is not possible to secure a BAA with all third-party providers. Because of this, we are unable to provide voicemail transcription for customers with HIPAA compliance needs.

As mentioned in the question above, alert emails are modified to ensure no PHI is included. For call alerts, this means the caller's name and phone number will not be included, and the recording link (if applicable) will require a login. Text message and lead capture alerts will primarily consist of a link back to CallRail for reviewing the content. Note that since Notification Only users cannot log in, they will only be able to see alerts about when these events happen. If these users need access to PHI, they will need to be prompted to Client Reporting users.

How are integrations handled with HIPAA regulations?

Third-Party integrations are available to use with CallRail. It should be noted that your data will leave CallRail, if integrations are used, and due diligence should be applied with the 3rd party to ensure you are in compliance. You may need to sign a BAA with the 3rd party as well.

What protections exist if I don't have a Business Associate Agreement (BAA) on file with CallRail?

CallRail is confident in its security, even without a BAA in place. However, use of CallRail involving PHI without a BAA in place is strictly prohibited by the Terms of Service. In that case, no legal protections are afforded, which places significant financial and legal liability on the healthcare provider. In addition, the extra security measures enabled for Healthcare customers cannot be activated without a BAA and healthcare plan.

Does CallRail maintain a BAA with any third-parties?

Yes, CallRail maintains Business Associate Agreements with applicable third-parties.

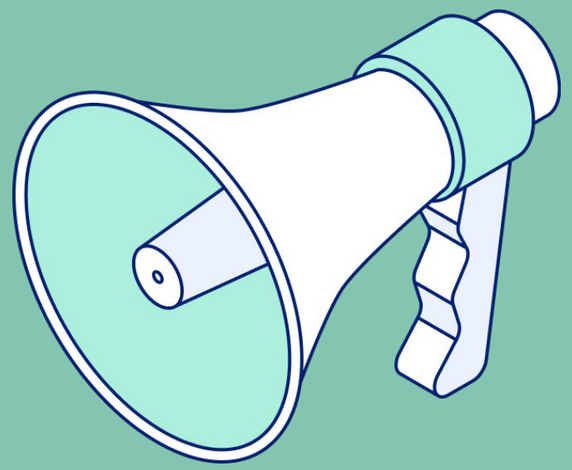
Does CallRail maintain access logs?

Yes, CallRail logs all access to the application with the logged-in user, timestamp, and IP address. Any changes to data and configuration are logged for audit purposes as well. In the case of a suspected breach or misuse, this audit log can provide a confirmed history of access.

This data is highly technical, and therefore not currently available within the application. Access to this data can be obtained by contacting Support. For complex requests, a research fee may apply.

Can I simply prevent my call tracking provider from gaining access to PHI?

A call tracking provider must handle both the source caller ID and the destination phone number in order to route a call, therefore the provider will have access to PHI.



Conclusion

Call tracking has numerous benefits but must be done in accordance with the laws for entities covered by HIPAA and HITECH. CallRail has the expertise to provide world-class call tracking for those with compliance needs.

Legal Disclaimer

The materials in this white paper are provided for informational purposes only and do not constitute legal advice. Transmission of the information is not intended to create, and the receipt does not constitute, an attorney-client relationship between sender and receiver. The information is offered only for general informational and educational purposes and does not constitute legal advice or legal opinions. You should not act or rely on any information contained in this white paper without first seeking the advice of an attorney. All risk of loss or damage is solely that of the user and the company disclaims any liability thereof.

CallRail

If you have any questions about HIPAA compliance or CallRail healthcare plans, please reach out to our team at (866) 208-8055 or sales@callrail.com

Try CallRail for free