CallRail

CallRail and HIPAA compliant call tracking

Keep your patients' protected health information secure

CallRail helps businesses and marketers continue to close the attribution gap by tracking inbound phone calls and form submissions from the marketing sources that drove them. But with that tracking comes a great responsibility, especially in the healthcare industry.

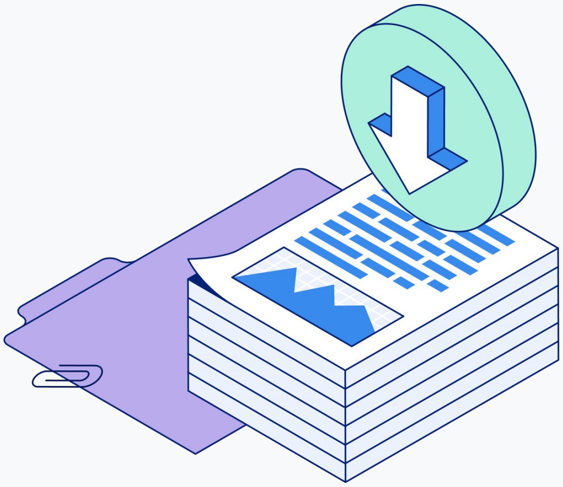
From scheduling appointments to billing, referrals, and prescription refills, private information can be communicated over the phone between patients and their healthcare provider. This information is protected under the Health Insurance Portability and Accountability Act (HIPAA) and its expansion, Health 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 the data from these calls stay secure.

CallRail has heard from many healthcare businesses concerned about online tracking technology and the steps needed to be taken to ensure compliance outlined by The Office for Civil Rights (OCR) in their December 2022 bulletin.[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 has you covered. We take 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.

Managing HIPAA compliance can be daunting. Leveraging these key capabilities, along with maintaining strong internal data practices, can help mitigate your compliance woes while allowing your practice to experience the many benefits of call tracking.



How CallRail keeps Protected Health Information (PHI) secure

Annual attestation to confirm compliance

Third-party audit of CallRail's practices
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.

The 4 HIPAA technical safeguards required for call tracking data:[3]

1. **Access Controls**
Technical policies and procedures for only authorized personnel to access Personal Health Information (PHI)

2. **Audit Controls**
Enable the ability to track and report all access to data

3. **Integrity Controls**
Ensure data cannot be altered or destroyed

4. **Transmission Security**
Guard against unauthorized access being transmitted

Access Controls

All data encrypted "at rest"
All call records, web visitor sessions, and call routing data are fully encrypted when stored on disk. This data is seamlessly decrypted as-needed for reporting purposes when accessed by the customer. These precautions protect the data even if hard drives fail, or are decommissioned or stolen.

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.

Firewalls and private network gaps
The databases, application servers, and other machines responsible for routing calls through CallRail 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.

Audit Controls

Full audit history
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.

Integrity Controls

Protection for external systems
CallRail prevents transmissions of call details considered Protected Health Information, like call recordings and caller ID, to external systems that aren't considered in compliance with HIPAA requirements and instead provides a link that requires the user to log in to review the information.

Transmission Security

All data encrypted "in transit"
All access to CallRail is encrypted via SSL to protect data from interception on network points between the user and CallRail.

References:

1. https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html
2. https://www.nelsonmullins.com/idea_exchange/blogs/healthcare_essentials/data_privacy_and_security/key-strategies-for-hipaa-compliant-use-of-online-tracking-technologies#_ftnref3
3. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html