HIPAA Checklist

CallTrackingMetrics

Maintain compliance with the regulations of HIPAA and HITECH while still leveraging critical data for your marketing and sales departments.

Requirements:

- ☐ **Check your plan:** You must be on the Connect, Growth, Advanced, or Enterprise plan to be HIPAA compliant.
- ☐ **Business Associate Agreement (BAA):** Contact us at info@calltrackingmetrics.com to request a BAA.
- ☐ **Tracking numbers:** Do not use tracking numbers that are marked as "not eligible for HIPAA compliance". Non HIPAA numbers will be marked with an asterisk on the Buy Numbers page as well as the Tracking Numbers page in your account.
- ☐ **Individual logins:** Each individual user accessing HIPAA accounts must have their own unique login for CTM.
- ☐ **User security:** Within Agency Settings, navigate to "Security" area and configure the following:
  - Logout users automatically after no more than 15 minutes of idle connection
  - Enable two factor authentication to ask for verification code every time or every 30 days
  - Check the box to require a user login to access call recordings
- ☐ **Encrypt call recordings:** If recording phone calls, you must enable encrypted call recordings and encrypted call recording storage in your account settings.
- ☐ **Secure Call Transcriptions:** If you are using transcriptions and expect sensitive information such as Social Security numbers or personal phone numbers to be exchanged, you need to enable Secure Call Transcriptions which will automatically detect the presence of that information in your interactions and will redact them from your recordings and transcriptions.

Additional Recommendations:

- ☐ **Enable automatic redaction** on your account to manage how much and how long information is being stored. Redaction can be configured to occur daily or every 30, 60, or 90 days, or it can be done manually for an individual call or text.
- ☐ **Avoid moving PHI out of CTM:** Avoid configuring triggers, notifications, or exports that move PHI out of CallTrackingMetrics into emails or text messages. If choosing to use any of these features, it is your responsibility to ensure security of the information once it leaves CallTrackingMetrics. For example:
  - When using SMS services on CTM, do not include PHI in the body of your text messages.
  - If using post call notifications, be sure to remove fields that could contain unsecured PHI from your notifications
  - When exporting the call log, remove any fields that contain unsecured access to PHI
- ☐ **Caller ID:** Consider turning off Caller ID in Call Settings if you do not need to collect the name or location of your callers, and avoid using Enhanced Caller ID if you do not need to collect that information.
- ☐ **Be mindful of third party services:** Integrations with third party services enable customers to link CallTrackingMetrics with external services such as Salesforce, Hubspot, or Facebook. It is your responsibility to ensure that any third party services or applications you choose to integrate with your CTM account are used in a HIPAA compliant manner.

This checklist is meant to serve as a guide to help you maintain compliance with HIPAA while using CallTrackingMetrics and is not a substitute for legal advice. You are solely responsible for identifying and configuring all HIPAA Accounts. You may need to make additional adjustments in your account based on your particular use case. Find more information on the HIPAA website.