Security and Privacy Management

CallTrackingMetrics

CallTrackingMetrics.com | 800-577-1872 | info@calltrackingmetrics.com

Introduction

Thousands of companies around the world rely on CallTrackingMetrics' cloud communications platform to exchange millions of calls and messages.

Providing reliable communication channels is only the first step. These communications must also follow the latest security best practices and comply with strict privacy regulations and corporate policies. The information contained in this document is intended to provide transparency on CallTrackingMetrics' security processes.

CallTrackingMetrics' (CTM's) Security and Privacy Program follows a streamlined framework based on NIST 800-30 Rev. 1 guidance. The program was initially developed to adhere to the Meaningful Use criteria and the HIPAA HITECH Express regulations. In early 2018, in addition to our HIPAA focused risk management work, we also included program updates to comply with The General Data Protection Regulation (GDPR) which went into effect on May 25, 2018 and the California Consumer Privacy Act (CCPA) which goes into effect on January 1, 2020.

Our initial process used a streamlined risk analysis questionnaire to establish the baseline system characterization, threat, vulnerability, and existing controls. Based on threat and risk profiles, a risk management plan was prepared to guide the implementation of critical risk abatement and security management functions as needed. Fundamental procedures were established to manage the initial risk remediation and are continued in an ongoing program of risk assessment, analysis, and remediation.

While security is a high priority for our whole team, a dedicated Security Team manages CallTrackingMetrics' Program, with a Security and Compliance Officer leading it. Information security policies and standards are approved by management.

Compliance Activities

The following activities are completed as part of CTM's Security Program:

1. Inventory of all software applications, hardware, network components, databases, and data transfers
2. Risk assessments
3. Access management
4. Security awareness training
5. Security and privacy policies and procedures
6. Plans including risk management, incident response, contingency, and physical security
7. Security monitoring and incident response
8. Third party security

Security, Risk, and Control Areas

The CallTrackingMetrics Security Program focuses on the following risk and control areas:

1. **Governance Strategy:** A strong top-down security culture at CTM reduces the risk of unauthorized activities and data breaches.
    a. An information security strategy and key goals are defined and communicated to all stakeholders across the organization.
    b. An information risk management program document address keys risks that CTM faces in the current environment.
    c. A Security and Privacy Compliance Officer manages the program.
2. **Security Risk Management:** Security risks have been identified and managed to mitigate potential negative effects in a programmatic way.
    a. A formal information security risk and compliance program manages risk to an acceptable level and compliance with applicable regulatory requirements (e.g. HIPAA Security Rule, HITECH, GDPR, CCPA etc.) is implemented.
    b. Risk assessments occur on a recurring basis to identify security risks.
3. **Policies and Procedures:** Policies and procedures have been implemented to provide a security implementation and management foundation. Business continuity has been tested to ensure readiness in the event of a breach or emergency to reduce financial, operational, and reputational risk.
4. **3rd Party Security:** Third-parties used by CallTrackingMetrics are assessed before onboarding to validate that prospective third parties meet CallTrackingMetrics security requirements.
    a. CTM has implemented a process to ensure that any organization working with CTM that touches Personal Data or PHI are also HIPAA, CCPA and GDPR compliant.
    b. Once a relationship has been established, CallTrackingMetrics periodically reviews security and business continuity concerns at existing third parties. The program takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.
    c. CallTrackingMetrics ensures that data is returned and/or deleted at the end of a vendor relationship.
5. **Access Controls:** CTM has a limited number of staff, often performing multiple duties. CTM has implemented an ongoing review of access and activity logs to ensure individuals are only performing authorized activities.
    a. CallTrackingMetrics logs high risk actions and changes in the production network. Changes are reviewed before moving into a staging environment where it is further tested before finally being deployed into production. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change occurring.

6. **Network Management:** Since CTM provides a service to others, the integrity of its systems, networks, and data is critical. CTM monitors its internal network as well as those of any third party service providers.

    a. Direct access to infrastructure, networks, and data is minimized to the greatest extent possible (principle of least privilege (POLP)). Where possible, control planes are used to manage services running in production in order to reduce direct access to host infrastructure, networks, and data. Direct access to production resources is restricted to only the employees requiring access. It requires approval, strong multi-factor authentication, and access via a bastion host.

    b. CallTrackingMetrics production environments, in which any customer data and/or customer-facing applications reside, are logically isolated networks. Production and non-production networks (i.e. staging, test, development) are segregated. All network access to production hosts is restricted using firewalls and other access controls to only allow authorized services to interact with the production environments.

7. **Data Protection Management:** CTM has implemented security controls to safeguard data and decrease the probability of unauthorized access and data leaks.

    a. Laptops, desktops, mobile devices, data backups, and applications/databases that contain data are encrypted.

    b. Electronic data exchanged (received and/or sent) is in an encrypted format, both internally and with external parties.

8. **Asset Management:** CTM regularly updates all software to reduce the risk that application infrastructure and application software may not have the latest security patches that could impact the availability of systems and data. The presence of malware on assets that could infect and disable the entire network is monitored.

9. **Training and Awareness:** All new CallTrackingMetrics employees attend a Security Training during the onboarding process. In addition, all CallTrackingMetrics must take CTM Security and Privacy training once a year which covers the policies, security best practices, and privacy principles. The Compliance Team provides continuous communication on emerging threats and communicates with the employees regularly.

10. **Contingency Planning:** Our implemented contingency plan reduces the risk of CTM being unable to resume normal operations after a disaster or emergency.

    a. A business impact analysis is conducted.

    b. Business continuity and disaster recovery plans are in place and regularly reviewed and updated.

    c. Hosting our services on Amazon Web Services (AWS) gives CallTrackingMetrics the ability to remain resilient globally even if one location goes down. AWS spans multiple geographic regions and availability zones, which allows CallTrackingMetrics servers to remain resilient in the event of most failure modes, including natural disasters or system failures.

11. **Backup systems for critical applications** are tested to ensure there is adequate capacity to store relevant information and that the ability to restore critical data is in place.

    a. CallTrackingMetrics performs regular backups of CallTrackingMetrics account information, call records, call recordings, and other critical data to encrypted local storage and cloud storage. All backups are encrypted in transit and at rest using strong encryption. CallTrackingMetrics supports TLS 1.0, 1.1 and 1.2 to encrypt traffic.

12. **Continuous Monitoring and Response Program:** Active monitoring and regular reviews of logs have been implemented to proactively identify issues and problems and reduce the risk of negative consequences to the organization.

    a. CallTrackingMetrics maintains an incident response program in accordance with NIST 800-61. The program defines conditions under which security incidents are classified and triaged. The Security Team assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events.

    b. Security logs are maintained for 180 days. Acccess to these logs is limited to the Security Team.

13. **Physical Security:** Physical security controls are in place to reduce the likelihood of unauthorized access or security incidents (e.g. theft).

    a. CallTrackingMetrics leverages AWS data centers for all production systems and customer data. AWS follows industry best practices and complies with an impressive array of standards. AWS complies with leading security policies and frameworks including SSAE 16, SOC framework, ISO 27001 and PCI DSS. For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

    b. Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. Direct access to production resources is restricted to employees requiring access and requires approval, strong multi-factor authentication and access via a bastion host.

    c. The CallTrackingMetrics production environment is a logically isolated Virtual Private Cloud (VPC). Production and non-production networks are segregated. All network access between production hosts is restricted using firewalls to only allow authorized services to interact in the production network.

    d. CallTrackingMetrics has a security program in place that manages access to our offices, visitors, and overall office security. All access to our office is restricted to employees and logged visitors.

14. **People Security:** We have implemented processes to ensure we're bringing in the right people and keeping them up to date on the latest security trends.

    a. All candidates in the USA must pass stringent background checks by a third party before being offered a position. These checks include SSN trace, criminal county search, multi-state instant criminal search, National Sex Offenders Public Registry, professional references, and education verification.

    b. All new CallTrackingMetrics employees attend a "Security 101" training during the onboarding process. In addition, all employees must take the annual CallTrackingMetrics Security Training once a year which covers the Information Security Policies, security best practices, and privacy principles.

    c. The Security Team provides continuous communication on emerging threats and communicates with the company regularly.

15. **Account Security:** CallTrackingMetrics secures accounts using industry best practice methods to salt and repeatedly hash credentials before storing. Users can also add another layer of security to their account using two-factor authentication for the CallTrackingMetrics application.

Ongoing Risk Management Initiatives

In addition to regular risk assessments, CallTrackingMetrics Security Program focuses on ongoing high priority initiatives to reduce risk.

People

- Annually review required information security roles and responsibilities
- Annually review staff and contractor access rights to maintain minimally required access

Governance

- Annually review the information security program supported by leadership which includes key program components (vision and strategy, communications, etc.) to manage the changing technology landscape
- Conduct periodic security and privacy awareness training and hot topic notifications

Information Security Risk Management

- Ongoing monitoring and annual review to identify and remediate key information security risks and data breach prevention
- Periodically monitor and remediate key information system controls

Information Security Function

Update, review, and approve information security policies, procedures, and plans on an annual basis

Data Security

Continuously monitor Personal Data and PHI data use, transmission, dissemination, and destruction policies and procedures

Questions?

For further details and steps to secure your CallTrackingMetrics account, check out our help center which provides additional guidance for customers needing to be HIPAA, GDPR, CCPA and PCI compliant. If you have more questions or need more detailed answers, contact our support team at info@calltrackingmetrics.com and we would be happy to help you.

Help Center: calltrackingmetrics.com/support
Call us: 800.577.1872
Email support: info@calltrackingmetrics.com