Information Security Summary

Effective Date/Last Revised: January 30, 2020

dialogtech

This high-level overview of DialogTech's Information Security practices and standards is intended to explain the company's approach to key data security and privacy concerns that are frequently raised by security-conscious customers.

DialogTech knows that all client data should be handled with the utmost care to preserve data security and client trust. The company follows industry best practices to ensure that DialogTech only uses industry-leading available encryption, physical, and logical security standards. DialogTech also keeps up to date on all of the latest security threats and are quick to mitigate any potential vulnerabilities. For example, DialogTech is PCI-, HIPAA-, and HITECH-compliant and continues to expand and strengthen their security initiatives, awareness, and practices.

It is also important to remember that while DialogTech delivers high-value services to its clients, the company does not impact clients' critical systems. The client data that DialogTech comes into possession of is both transient and limited in scope and nature. As such, DialogTech is a low-risk data custodian.

DialogTech has also implemented a California Consumer Protection Act (CCPA) compliance program to assist clients with consumer data access and deletion requests. DialogTech is committed to protecting its client data and will continue to expand and strengthen its security initiatives, awareness, and practices.

Policies and Standards

With the number of clients DialogTech has in the healthcare industry, DialogTech has adopted HIPAA-oriented policies and training that also support their PCI-DSS compliance as a Level 1 Service Provider. The company's primary focus is on the confidentiality and privacy of end consumers whose personally identifiable information may be collected on behalf of DialogTech's clients. DialogTech leverages the same standards across its non-HIPAA client base, to ensure that all of DialogTech's clients' data is protected. These policies address the technical, administrative and physical protections of DialogTech. DialogTech requires all employees to attend mandatory HIPAA training and to read and acknowledge all policies. DialogTech also tracks compliance and provides ongoing privacy training.

DialogTech requires all employees and anyone who has access to any of its networks and data centers to undergo a thorough background check that verifies employment, education, criminal, and a credit background check before they begin employment. Furthermore, the company only employs services of third-party contractors that undergo background checks as well. DialogTech also requires all contractors to agree to a non-disclosure agreement and Business Associate Agreements, when appropriate, before conducting business.

Data Collected

Depending on which DialogTech services a client uses, DialogTech has the ability to collect a variety of client data. This includes consumer call history, caller ID, call transcriptions, browsing history, and IP addresses. If features such as call recording, call transcriptions, and reverse lookup are enabled, DialogTech will collect those call recordings, call transcriptions, and phone number owner's name and address, which may be considered as personally identifiable information (PII). Collection around any or all of these data components can be managed to best fit DialogTech's clients' security needs.

DialogTech does not share any client data with third parties. DialogTech specifies in its contracts that DialogTech's clients own any data pertaining to their consumers collected on their behalf. However, DialogTech does utilize the services of several third-party vendors to enhance the company's offerings, and they have access to a subset of this data. This includes vendors who provide caller ID lookup. DialogTech performs due diligence to enter into contracts with highly reputable vendors that put in place protections regarding their access and use of data.

Data Security

To ensure that client information is kept confidential, all data at rest is stored in DialogTech's SSAE-16 Certified SOC Type II compliant data centers using industry best practices for encryption at rest. This includes all production data as well as backups. Data in transit is encrypted using the most advanced cryptographic techniques available, and DialogTech is vigilant to cease the support of protocols and technologies that are no longer considered secure. DialogTech's security measures, including encryption at rest, encryption in motion, and access limited on the basis of least privilege, extends to our corporate office as well.

DialogTech provides a number of options that clients can enable to enhance the security levels. DialogTech is a PCI Level 1 Service Provider. This means that the DialogTech platform as a service is PCI DSS-compliant — including call recordings, call transcriptions, and AI-driven conversation analytics. Marketers can leverage the full benefits of DialogTech with confidence, knowing their data is protected by the only call tracking provider whose PCI DSS-compliance is in-house, which means DialogTech doesn't expose data to third parties.

The DialogTech Private feature provides the option for clients to turn off call recording, call transcriptions, and to obfuscate caller ID information. DialogTech's flexible API gives the option for customers to download their recordings and automatically delete them from DialogTech's servers.

In addition, DialogTech's data centers implement the utmost care with regard to physical security. Both premises provide 24/7 security and monitoring, and only approved DialogTech employees are permitted to access the data centers and physical servers. DialogTech also only uses highly reputable payment processors to process all client payment information to avoid storing credit card information or other sensitive payment data on DialogTech owned and operated servers.

Access Controls

Following the principle of least privilege, DialogTech only allows access to client data by those who require that access to perform their job duties. DialogTech frequently reviews access controls to verify that all accounts have the minimum necessary access rights. Furthermore, DialogTech has a strict password and login policy that requires all DialogTech employees to use strong passwords rotated frequently and locks employees out of their account after a number of failed attempts. Access to modify any records is severely limited, and call records and other related information are machine-generated and can only be modified by approved users.

DialogTech provides a number of tools clients can use to control access to their accounts and data by their employees. Each client has the ability to manage their own user base as needed, and the ability to generate and revoke API key pairs as well. DialogTech's authorization system allows the creation of users with limited access, allowing them to see a subset of the data in their account that is relevant to them, without sharing all of their data. Additionally, DialogTech's tools allow clients to configure their own password restrictions, timeouts, and reuse policies under the condition that their custom policies are as strong or stronger than DialogTech's requirements.

Third-Party Auditing and Penetration Testing

DialogTech partners with industry-leading security experts to perform external and internal tests and scans on all DialogTech applications and networks on a regular basis, and all issues are remediated immediately. DialogTech leverages additional tools in development and test environments to check for vulnerabilities and to ensure issues are resolved before promotion to production.

Telco Security

DialogTech's extensive telco infrastructure requires the business to approach security on its telephony infrastructure as they would any other network. Every telco endpoint is behind an SBC, which serves as a firewall for DialogTech's telecom networks. Additionally, DialogTech makes use of dedicated circuits for their carrier connections, ensuring the highest possible call quality while maintaining the security of the conversation.

Disaster Prevention and Recovery

DialogTech's 24/7 operations staff have multiple systems and monitors to detect catastrophic failures and to ensure immediate action. In disaster recovery scenarios, DialogTech teams are focused on restoring clients' mission-critical systems first, with a focus on telephony connectivity. In the case of total data center failure, teams can restore telephony services within 15 minutes for many clients' telephony configurations.

Conclusion

DialogTech knows data is critical to its clients' businesses, and DialogTech places the highest priority on the privacy and security of their systems. DialogTech is happy to answer any questions clients may have on these topics and has a team solely dedicated to addressing these concerns. In addition, DialogTech makes proactive efforts to sign Business Associate Agreements ("BAA's") for any business that may be a HIPAA covered entity and completes appropriate security questionnaires for clients or prospective clients upon request.