Information Security Summary

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

At DialogTech, we know that all customer data should be handled with the utmost care to preserve data security and customer trust. We follow industry best practices to ensure that we use only the industry leading available encryption standards, physical, and logical security. We also keep up-to-date on all of the latest security threats and are quick to mitigate any potential vulnerabilities. DialogTech is fully HIPAA and HITECH compliant and we continue to expand and strengthen our security initiatives, awareness, and practices.

Policies and Standards

With the number of customers we have in the Healthcare industry, we have adopted HIPAA oriented policies and training. Our primary focus is on the confidentiality and privacy of end consumers whose personally identifiable information may be collected on behalf of our customers. We leverage the same standards across our non-HIPAA customer base, to ensure that all of our customers' data is protected. These policies address our technical, administrative and physical protections. We not only require all employees to attend mandatory HIPAA training, read and acknowledge the policies, but we track compliance and provide ongoing privacy trainings.

We require all employees and anyone who has access to any of our networks and data centers to undergo a thorough background check that verifies employment/education, criminal, and credit background check before they begin employment. Furthermore, we only employ the services from third-party contractors that perform background checks as well. We also require all contractors to sign and agree to a non-disclosure agreement before conducting business with them.

Data Collected

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

We do not share any customer data with third parties, and specify in our contracts that our customers own any data pertaining to their consumers we collect on their behalf. However, we do utilize the services of several third party vendors to enhance our offerings, and they have access to a subset of this data. This includes whitepages.com who provides caller ID lookup. We perform 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 our customer information is kept confidential, all data at rest is stored in our SSAE-16 Certified SOC Type II compliant Data Centers using AES 256-bit encryption. This includes all production data as well as our backups. Data in transit is encrypted using 2048-bit keys for all transfers between our offices and the datacenters, and between our data centers and our customers. In addition, we have disabled all insecure protocols. For example, we require a minimum connection of TLS 1.1 and above enabled with 1.0 disabled on our platform and internal networks.

We provide a number of options that our customers can enable to enhance the security levels. Our DT Private feature provides the option for our customers to turn off call recording, call transcriptions, and to obfuscate caller ID information. We also provide the option to mask any PII in our call transcriptions. Our flexible API gives the option for our customers to download their recordings and automatically delete them from our servers.

In addition, our data centers implement the utmost care in 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. We also use PayPal to process all customer payment information to avoid storing credit card or other sensitive payment data on DialogTech owned and operated servers.

Access Controls

Following the principle of least privilege, we only allow those who need access to an individual customer's data on a need to know basis. This means only the DialogTech employees who are required to support a specific customer's needs will have the permissions and access rights to view a customer's information. We frequently review access controls to verify that all accounts only have the access rights to the data necessary. Furthermore, we have a strict password and login policy that requires all DialogTech employees to use strong passwords and locks employees out of account after three failed attempts. Access to modify any records is severely limited, and call records and other related information is machine-generated and can only be modified by approved users.

We provide a number of tools our customers can use to control access to their account and data by their employees. Each customer has the ability to manage their own user base as needed, and the ability to generate and revoke API key pairs as well. Our authorization system allows the creation of users with limited access, allowing them to see a subset of the data in your account that is relevant to them, without sharing all your data. Additionally, our tools allow our customers to configure their own password restrictions, timeouts, and reuse policies under the condition that their custom policies are equally or stronger than ours.

Third Party Auditing and Penetration Testing

DialogTech partners with industry leader TrustWave to perform assessments on all DialogTech networks on a monthly basis. TrustWave provides detailed reports outlining potential vulnerabilities that may need to be addressed that would potentially compromise customer information. Weekly, we run an intensive security scan using Portswigger's Burp Suite Professional on our customer portal. In addition, we perform manual penetration tests at the application and network levels at least four times a year. We are currently in the process of onboarding a vendor for performing semi-annual secure code reviews to ensure our product is following best security practices. In the event that any security vulnerabilities are brought to our attention, we make it our highest priority to mitigate and resolve them.

Telco Security

Our extensive telco infrastructure requires us to approach security on our telephony infrastructure as we would any other network. Every telco endpoint is behind an SBC, which serves as a firewall for our telecoms networks. For our SBCs we use an open source solution, FreeSWITCH, which analyzes our telephony traffic and ensures that only legitimate traffic is being generated on that network.

Disaster Prevention and Recovery

Our 24x7 operations staff have multiple systems and monitors to detect catastrophic failures and ensure immediate action. In disaster recovery scenarios, our teams are focused on restoring our customers' mission critical systems first, with a focus on telephony connectivity. In the case of total data center failure, our teams can restore telephony services within 15 minutes for many of our customer's telephony configurations.

Long Term Security Plans

Currently we have several Information Security related projects on our roadmap that we aim to have completed by mid-2018. We are evaluating third party vendors to obtain a SOC2 Type 1 certification. We understand that third party verification of our security controls is important for our customers and the SOC2 would document our controls and compliance with key regulations as well as our internal policies and customer requirements. In addition we have been in contact with several vendors for the deployment of a Web Access Firewall (WAF). This would provide an extra blanket of protection on our public facing customer portal and provide extra DoS protection to ensure the availability of our platform. Finally, we are evaluating various vendors for an IDS and SIEM solution. This would provide to us additional tools for the tracking and logging of our environment to ensure there is no authorized access.

Conclusion

We know your data is critical to your business, and we place the highest priority on the privacy and security of our systems. We are happy to answer any questions you may have on these topics and have a team solely dedicated to addressing those concerns. In addition we make proactive efforts to sign Business Associate Agreements ("BAA's") for any business that may be a HIPAA covered entity, and complete appropriate security questionnaires for customers or prospective customers upon request.