Operating Stitch in Compliance with HIPAA

Stitch utilizes Amazon Web Services (AWS) infrastructure to process customer data, and Stitch has entered into a Business Associate Agreement (BAA) with AWS to ensure that Stitch services are offered in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Stitch customers who wish to leverage this agreement and have Electronic Protected Health Information (ePHI) processed by Stitch must agree to perform the following steps to ensure the data is protected in accordance with AWS and government requirements.

First, the customer shall enter into a BAA with Stitch. This will ensure that both are protected and that the customers and Stitch's requirements are detailed in a legally binding document. This document will include security requirements, obligations, and breach reporting procedures. This can be done by contacting the Stitch sales team through the form at https://www.stitchdata.com/contact/.

Second, the customer must ensure that PHI is not present in metadata used by Stitch, including:

- User, account, and integration names
- For database sources: user, database, schema, table, and column names
- For web service sources: dataset and field names

The customer must also ensure that PHI is not transmitted in support requests to Stitch through any medium (including in-app messaging and email).

Third, the customer must only transmit PHI from the following HIPAA-compliant sources, configured as described:

- MySQL, MariaDB, Amazon Aurora MySQL Edition, Google Cloud SQL for MySQL, PostgreSQL, Amazon Aurora Postgres Edition, Google Cloud SQL for PostgreSQL, Microsoft SQL Server, Microsoft Azure SQL Database, MongoDB – either the SSH or SSL encryption options must be chosen to secure PHI, and the customer must ensure that their systems are appropriately patched and configured per industry-standard best practice to ensure a secure communication session.
- Salesforce.com – any configuration
- Zendesk – any configuration
- Desk.com – any configuration

It is acceptable to transmit both PHI and non-PHI data within the same Stitch account, as long as the account is configured according to this document and PHI is only transmitted from the above sources.

Fourth, the customer must only transmit PHI to the following HIPAA-compliant destinations:

- Amazon Redshift
- Snowflake
- Google BigQuery
- Postgres – either the SSH or SSL encryption options must be chose to secure PHI, and the customer must ensure that their systems are appropriately patched and configured per industry standard best practice to ensure a secure communication session.

Configuration of the customer data warehouse is the customer’s responsibility. Stitch only transmits data to the location and service the customer specifies. The customer shall ensure that this is a secured environment, configured in accordance with HIPAA requirements and compliant with industry-standard best practices. Stitch shall not be liable for any noncompliance associated with the data warehouse.

Fifth, customer-supplied credentials for Stitch to access their environment and to transmit data to the customer warehouse must be robust. Passwords must be complex and not easily guessed. Passwords should be unique to the Stitch service and shared only on a need-to-know basis.

Finally, the customer must activate the “Hide plain-text error messages in notification emails” setting in the Account Settings page of the Stitch web application. This ensures that PHI is not sent through email as part of an error message.