Affirmed Healthy

Customer Goals & Privacy Considerations

Affirmed Healthy offers a mix of solutions with flexible processes and data storage options depending on the customer goals.

Typical customer goals consist of one or more of the following:

Assessment Reporting

Issuing assessments to employees and students and having them complete the assessment, but not requiring health pass validation for entry.

Access Control

Controlling entry access by confirming that the Affirmed Healthy pass has been issued and is valid.

Contact Tracing

Ensuring Affirmed Healthy health passes are scanned and user data is saved to allow for contact tracing based on the time stamp of the pass or badge scan.

There are privacy considerations that align with each customer goal:

Protected data that is identified to the Customer

Protected data that is identified to Affirmed Healthy

Protected data retention policies for where and how long data is retained

Contact Us for a FREE trial

EMAIL
info@affirmedhealthy.com

PHONE
1. 833. 823. 3476

Affirmed Healthy considers three data classifications when considering privacy:

Consent Data

All customer goals require an initial consent to be collected by Affirmed Healthy. This data must be retained by Affirmed Healthy for compliance purposes.

Personal Data

The personal data that is collected is based on what data the customer wants to collect and personal data is not required for all customer goals. Personal data may include data such as the users first and last name and employee ID. This data may be retained for various time periods based on if it is intended to be used for contact tracing.

Health Data

All customer goals require health data to be collected as this includes the results from the health assessment. Health data is also customizable by the customer and may include confirmation of any recent COVID-19 tests and/or confirmation of symptoms and temperature. Health data may be retained by Affirmed Healthy for a set retention period and/or the customer or may not be retained at all by Affirmed Healthy and/or the customer once the pass is issued.

The following data classifications are required by goal:

Assessment Reporting

Consent and health data is required and typically reporting requires personal data to be collected.

Access Control

Consent and health data is required, but access control may be implemented with or without personal data collection or retention.

Contact Tracing

Consent and health data is required. Typically contact tracing requires personal data to be collected and retained to allow for contact if needed.

Contact Us for a FREE trial

EMAIL
info@affirmedhealthy.com

PHONE
1. 833. 823. 3476

Affirmed Healthy Access Control Options:

Access Control Option 1: Affirmed + De-identified Access

Employees are issued de-identified credentials after affirming their health. Access control verifies the credential but does not have an identity relationship.

PRO & CON

- ✓ No PII data exposed.
- ✗ No reporting or contact tracing, no identity verification.

Access Control Option 2: Affirmed + Identified Access

Employees are issued credentials linked to their person after affirming their health. Access control verifies the credential and records the identity.

PRO & CON

- ✓ Contact Tracing, Identity verification.
- ✗ PII data is stored with health data.

Access Control Option 3: Affirmed Relational Access

Employees provide Affirmed Healthy their employee ID number. They are not issued credentials. Instead Affirmed Healthy associates the health pass with the employee ID via API or web hook. Their employee ID is activated on the barcode scanner daily.

PRO & CON

- ✓ Some PII data exposed.
- ✗ Needs a barcoded badge/ID, Employee ID is shared.

Contact Us for a FREE trial

EMAIL
info@affirmedhealthy.com

PHONE
1. 833. 823. 3476