SHARED RESPONSIBILITY SECURITY

Updated: July 13, 2021

Alida.

NOTICES

This document is provided for informational purposes only. It represents Alida's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Alida's products or services. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Alida, its affiliates, suppliers or licensors. The responsibilities and liabilities of Alida to its customers are controlled by Alida agreements.

The terms set out in the above notice may be changed by Alida without notice or consent.

Customers should ensure they are reviewing the latest version of the document as it may be updated at any time without notice. The latest version of this document is always available on our website at: https://www.alida.com/hubfs/shared_responsibility_security.pdf

TABLE OF CONTENTS

OVERVIEW

This document covers important security and privacy considerations when using Alida's products and services.

STUDIES

Our Insight Community Platform provides a flexible platform for collecting information from community members. It is important when designing studies that survey authors ensure the questions asked comply with their Insight Communities privacy policy, your company policy and any relevant local privacy laws. Users should not upload any data to their Insight Community that requires specialized access protection (such as Bank Account Numbers, Social Insurance Numbers or the equivalent).

Customers who are required to comply with HIPAA legislation should be aware that Member Image Upload questions are hosted in AWS by a third party that is not covered by a Business Associate Agreement.

Customers in the European Union should be aware that the image Member Image Upload questions are hosted in AWS USA by a third party SaaS provider that has not entered into Standard Contract Clauses however that third party operates out of Israel, which has equivalency under EUJC rulings and therefore is not required to enter into Standard Contract Clauses. However, that third party does have inter-company data transfer agreements.

SPARQ 1 SPECIFICS

Sparq 1 provides an advanced scripting capability. Users who script or otherwise customize the behavior of their Sparq 1 install as responsible for the quality of their own code and ensuring the comply with the secure coding guidelines of their own company.

There are additional data protection features that may be enabled upon request which include:

- IP address based access restrictions to the administrative portal
- Protection against Cross Frame Scripting (by disabling iframe embedding)
- Data Purge which allows for the anonymization of community member data when it meets certain criteria

SPARQ 2 AND SPARQ 3 SPECIFICS

Sparq 2 and Sparq 3 also includes the ability to utilize external survey tools; customers are responsible for the security of such integrations as they are outside Alida's control.

The integrated Discussion Forum's capability is an open discussion forum and customers should be conscious of which topics they raise in their discussion forums with their community members as once invited into a discussion there are no additional access controls and all members of a single discussion can see the content of other discussion participants.

API ACCESS

Requests to the APIs are routed through Alida's central API gateway at api.visioncritical.com which is currently located in Oregon, USA. Customers should only make use of this central API gateway if permitted by their privacy policy, data export laws or any other regulations that specifically apply to the type of data being sent. Alida also provides the following region-specific API gateways:

api.na1.alida.com

api.na2.alida.com

api.eu1.alida.com

api.eu2.alida.com

api.ap2.alida.com

Customers that cannot make use of the Central API gateway due to their privacy policy, laws or regulations should switch to the new gateways. Customers are solely responsible for their use of the API and handling of API credentials; customers should create dedicated API access accounts for managing and auditing access to the platform.

REGULATORY MATTERS

The API Gateway is not covered by Alida’s Business Associate Agreement. Personal Health Information as defined by the USA’s Health Insurance Portability and Accountability Act should not be sent via the API. Deidentified data extracted from Personal Health Information can be sent to the API.

The API Gateway is covered by Standard Contractual Clauses that Alida provides to its customers which process data from European subjects.

UPDATES

DATE	CHANGE SUMMARY
July 13, 2021	Updated API Access section Rebranded to align with Alida brand guidelines
March 16, 2017	Updated incorrect location of gateway – now correct as Oregon Clarified language in API Access Clarified language in Regulatory matters Renamed Sparq to Sparq 1 and Sparq Next Gen to Sparq 2 and Sparq 3 Fixed broken link to document in Notices
February 16, 2017	Gateway moved to Virginia, USA EU data protection addressed
August 1, 2016	First published