Nayya

Data Privacy and Information Security Program

Our stance on data privacy

At Nayya, our commitment to data privacy and security is at the core of everything we do. Nayya follows generally accepted industry standards and maintains reasonable and appropriate safeguards to ensure the security, availability, integrity, confidentiality and privacy of the information in Nayya's possession.

Nayya is SOC 2 Type 2, HIPAA, and CCPA compliant so users can rest assured that personal data is well protected. Further, Nayya partners with a 3rd party vendor to actively monitor our controls to ensure security and compliance are continuously operating effectively.

Additional web application and network penetration testing is performed on a regularly scheduled basis in accordance with Nayya's regular compliance activities. Third party providers are subject to similar controls review.

Our usage of personal data

We use personal information for the following purposes and as otherwise described in this Privacy Policy or at the time of collection:

1. Provide, operate and improve the Service
2. Establish and maintain user profiles on the Service
3. Manage the security features of the Service
4. Understand needs and interests, and personalize experiences with the Service
5. Provide support and maintenance for the Service
6. Utilization to analyze and improve the Service

Any personal user information collected by Nayya will never be shared with a user's employer.

Identity Access Management

Authentication
Employees and users authenticate via SAML v2.0 based Single-Sign-On (SSO).

Authorization
The Application supports a multi-user, multi-tenant environment. Users are limited to accessing their own personal data, which may include but is not limited to data linked through third party account linkage and data captured from app usage.

Personal information collected by Nayya is stored in secure operating environments that are not available to the public. Nayya has technical, administrative, and physical security measures in place to protect users' personal information from unauthorized access and improper use. Authorization is enforced to prevent improper user access through mechanisms such as link manipulation or rights elevation.

Systems are designed to operate with the minimum amount of privilege necessary. This principle of "least access privilege" applies to all employees and users and is audited according to our policies and procedures.

Password management
Nayya's employees are required to generate and store strong secure passwords in a corporate provided password manager. If a user created an account using Single-Sign-On (SSO), passwords are stored by their respective authentication platform.

Frequently asked questions

Encryption
The platform supports 256-bit Transport Layer Security (TLS) 1.2 for data encryption in transit. Data at rest is encrypted using Advanced Encryption Standard (AES) 256.

Data Retention
All user data, including personally identifiable information (PII), will be retained in accordance with Nayya's Data Management policy.

Anonymized and aggregated data may be retained for internal or marketing purposes.
If a user requests to delete their data, we will comply and delete that user's PII within 30 days.

Frequently asked questions cont'd

Server Security
The solution is hosted in AWS public cloud, within the United States only.
A multi-tier server architecture is in place to prevent unauthorized data access from any location.

Multiple layers of security have been designed into the solution, with APIs providing a layer of abstraction between the front-end and back-end. The failure of any single layer will not result in complete compromise of the system.

Trusted partners
Our partners' data security and privacy practices have been vetted by the Nayya IT team and they meet our own highly held security standards. The following outlines a more detailed view of our Partners' data practices:

- Password management: Nayya does not store user passwords
- Security/Encryption: To ensure users' data is secure, our partners follow industry-standard security measures, and they always encrypt any transmissions to and from Nayya
- Monitoring: Like the Nayya team, our partners continuously monitor for potential security breaches and system failures, to ensure users' information remains secure
- Data Retention: Partners will not retain, use, or sell any PII of users. They may use aggregated or de-identified data for internal, academic-research, or marketing purposes

More information is available upon request.

Monitoring and alerting practices
Nayya performs proactive monitoring and alerting to detect any suspicious, unusual and malicious activity as well as alerts and notifications to appropriate parties for immediate actioning.