Proprietary & Confidential

Nayya

System Description of the Platform

SOC 3

Relevant to Security

DECEMBER 16, 2020 TO DECEMBER 15, 2021

MOSSADAMS

Table of Contents

I. Independent Service Auditor’s Report 1

II. Nayya’s Assertion 3

III. Nayya’s Description of the Boundaries of Its Platform 4

A. System Overview 4

1. Services Provided 4
2. System Boundaries 5
3. Subservice Organizations 5
4. Infrastructure 5
5. Software 6
6. People 6
7. Data 7
8. Processes and Procedures 7

B. Principal Service Commitments and System Requirements 7

C. Complementary Subservice Organization Controls 8

D. Complementary User Entity Controls 10

I. Independent Service Auditor’s Report

Nayya Health, Inc.
57 E. 11th Street, 4th Floor
New York, NY 10003

To the Management of Nayya:

Scope

We have examined Nayya’s accompanying assertion in Section II titled “Nayya’s Assertion" (assertion) that the controls within Nayya’s Platform (system) were effective throughout the period , 2020 to , 2021, to provide reasonable assurance that Nayya’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Nayya uses a subservice organization for cloud hosting and infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nayya, to achieve Nayya's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nayya's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nayya, to achieve Nayya's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

Nayya is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Nayya’s service commitments and system requirements were achieved. Nayya has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Nayya is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Nayya's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Nayya's service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Nayya's Platform were effective throughout the period December 16, 2020 to December 15, 2021, to provide reasonable assurance that Nayya's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

San Francisco, California
May 5, 2022

II. Nayya’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nayya’s Platform (system) throughout the period December 16, 2020 to December 15, 2021 to provide reasonable assurance that Nayya’s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section III entitled “Nayya’s Description of the Boundaries of Its Platform” and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 16, 2020 to December 15, 2021, to provide reasonable assurance that Nayya’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*. Nayya’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III entitled “Nayya’s Description of the Boundaries of Its Platform”.

Nayya uses subservice organization AWS Elastic Container Service for cloud hosting and infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nayya, to achieve Nayya’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nayya’s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nayya, to achieve Nayya’s service commitments and system requirements based on the applicable trust services criteria. The description presents Nayya’s complementary user entity controls assumed in the design of Nayya’s controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 16, 2020 to December 15, 2021, to provide reasonable assurance that Nayya’s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Nayya's Description of the Boundaries of Its Platform

A. System Overview

1. Services Provided

COMPANY OVERVIEW

Nayya is an AI-based, "look-alike" recommendation tool that helps employees choose and use the optimal benefits package for them, given their specific financial, family, and employment situation. By merging proprietary, first-party information with curated, third-party data, Nayya micro-segments employees across demographic, psychographic, behavioral, and geospatial indicators, resulting in curated, scientific decision making.

A typical "open enrollment period" requires an employee to select the right mix of benefits, across hundreds total possible combinations, given their specific family, income, and health needs. This optimization problem is extremely difficult and leads to anxiety, hours of assessment, significant uncertainty with the final decision, and, typically, a sub-optimal decision that over-insures them in certain benefits and under-insures them on others. In the former situation, money is being taken out of the household as opposed to being spent on food, retirement, or student loans, when 80% of Americans are living paycheck to paycheck. In the latter, employees leave themselves exposed to the highest cause of bankruptcy in America today -- healthcare expenses.

Nayya helps solve this challenging optimization problem for employees. Nayya sits between the insurance carriers, benefit brokers, human capital management (HCM), benefit administration, employers, and pharmacy benefit managers (PBMs); and, through the AI, asks personalized questions to assess a particular employee's specific situation to create a data-driven, optimized recommendation based on historical insurance use, scenario-based risk scoring (e.g., commute or child activities), and "look-alike" analysis.

SYSTEM DESCRIPTION

Prior to open enrollment, Nayya partners with the employer, broker, and insurer to retrieve plan data, plan rates, and plan designs being offered by the employer. Nayya will often receive a demographic profile and employee census, both as point-in-time CSV transfers or real-time API integrations with the employer's HCM platform (e.g., ADP, Selerix, Workday).

During the open enrollment experience, Nayya will guide the employee user through a series of dynamic questions to learn about them and build a consumer profile. The questions are directed around the employee's demographic, family, financial wellness, medical history, psychographics, cost sensitivity, and risk. During this process, Nayya appends external third-party data about this individual (both individualized and aggregated data) to enhance the consumer profile and give the Nayya recommendation engine a more holistic view of the individual. After building the consumer profile, Nayya will recommend plans using "look-alike" data and risk modeling.

It's important to note that Nayya provides "decision support" during the enrollment experience but doesn't offer the enrollment experience itself. The employees typically complete enrollment on the employer's benefits administration software.

2. System Boundaries

The system boundaries for consideration within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting the Platform.

3. Subservice Organizations

Nayya uses AWS Elastic Container Service for cloud hosting and infrastructure. This subservice organization is excluded from the scope of this report; the controls it is expected to provide are included in the subsequent section titled *Complementary Subservice Organization Controls*.

4. Infrastructure

Nayya's Platform is a Software-as-a-Service (SaaS) cloud-based system. The primary components of the Platform are built on top of Amazon Web Services (AWS). The Platform is built using the following AWS services:

AWS Service	Function
Amazon API Gateway	Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale.
Amazon Elastic Compute Cloud (EC2)	Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud
Amazon Elastic Container Service (ECS)	Amazon ECS is a fully managed container orchestration service.
Amazon RDS	Amazon RDS is a managed relational database service for MySQL, PostgreSQL, MariaDB, Oracle BYOL, or SQL Server.
Amazon Simple Queue Service (SQS)	Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.
AWS CodeArtifact	AWS CodeArtifact is a fully managed artifact repository service that makes it easy for organizations of any size to securely store, publish, and share software packages used in their software development process.
AWS CodeDeploy	AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of computer services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers.

AWS Service	Function
AWS Lambda	AWS Lambda is a serverless, event-driven compute service that lets you run code for virtually any type of application or backend service without provisioning or managing servers.
AWS Simple Cloud Storage (S3)	Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

5. Software

The Platform is built using HTML / CSS and JavaScript for the front-end, which is backed by Ruby on Rails on the back end and PostgreSQL as the main application database. In addition, Python is used in the data layer, as well as GitHub, and Docker for the infrastructure.

Additionally, the following vendor software is used to help manage the Platform:

Vendor Software	Function
GitHub	GitHub provides hosting for software development version control using Git. GitHub provides access control and several other collaboration features such as bug tracking, feature requests, task management, and wikis for all projects.
Papertrail	Papertrail is a log management tool.

6. People

The control framework that supports Nayya's organizational environment starts with its executive team. The following are key roles involved in control implementation and maintenance:

- Chief Executive Officer (CEO)
- Chief Technology Officer (CTO)
- Security Officer
- Director of Engineering

Responsibility for Nayya's information security resides with the Security Officer. In addition to the overall governance provided by the executive team, the following teams play a key role in the execution of controls:

- *Engineering* – The Engineering team is responsible for software development.
- *Human Resources (HR)* – The HR team is responsible for employee onboarding, setting policies, and employee reviews.
- *Security* – The Security team is responsible for security of the applications and service data.

7. Data

Within the Platform, service data is name, email, address, income, demographic data, psychographic data, and data pertaining to ePHI.

8. Processes and Procedures

Nayya has developed and communicated to its personnel procedures to protect service data and the company's assets. Procedures are documented and updated on the company intranet to help ensure personnel are informed and equipped to perform their duties to preserve the security of the Platform and the service data.

These procedures include the following policies:

- Acceptable Use
- Asset Management
- Change Management
- Code of Conduct
- Encryption and Key Management
- Data Protection
- Incident Response
- Information Security
- Password
- Risk Assessment and Management
- System Access and Authorization Control
- Vendor Risk Management
- Vulnerability Management and Patch Program

B. Principal Service Commitments and System Requirements

Nayya designs its processes and procedures to meet its security objectives. Those objectives are based on the service commitments that Nayya makes to user entities and the financial, operational, and compliance requirements that Nayya has established for the Platform.

Security commitments to user entities and customers, and a description of the Platform, are documented within and communicated through the Nayya online Terms of Service when creating an account.

C. Complementary Subservice Organization Controls

Nayya's controls related to the Platform cover only a portion of overall internal control for each user entity of Nayya. It is not feasible for the criteria related to the Platform to be achieved solely by Nayya. Therefore, each user entity's internal controls must be evaluated in conjunction with Nayya's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	Complementary Subservice Organization Controls		Related Criteria
1	Access to hosted systems requires strong authentication mechanisms.	➤	**CC 6.1** **HIPAA §164.308(a)(5)(ii)(D)**
2	New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to being granted.	➤	**CC 6.1, CC 6.2, and CC 6.3** **HIPAA §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(3)(ii)(C), §164.308(a)(4)(i), §164.308(a)(4)(ii)(A), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.308(a)(5)(ii)(C), §164.308(a)(5)(ii)(D), §164.310(a)(2)(iii), §164.312(a)(2)(i), §164.312(a)(2)(ii), §164.312(d)**
3	Terminated user access permissions to hosted systems are removed in a timely manner.	➤	**CC 6.1, CC6.2, and CC 6.3** **HIPAA §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(3)(ii)(C), §164.308(a)(4)(i), §164.308(a)(4)(ii)(A), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.308(a)(5)(ii)(C), §164.308(a)(5)(ii)(D), §164.310(a)(2)(iii), §164.312(a)(2)(i), §164.312(a)(2)(ii), §164.312(d)**
4	User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.	➤	**CC 6.2 and CC 6.3** **HIPAA §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(3)(ii)(C), §164.308(a)(4)(i), §164.308(a)(4)(ii)(A), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.308(a)(5)(ii)(C), §164.308(a)(5)(ii)(D), §164.310(a)(2)(iii), §164.312(a)(2)(i), §164.312(a)(2)(ii), §164.312(d)**

Complementary Subservice Organization Controls		Related Criteria
5	Privileged access to hosted systems and the underlying data is restricted to appropriate users.	**CC 6.3 and CC 6.7** **HIPAA §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(3)(ii)(C), §164.308(a)(4)(i), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.308(a)(5)(ii)(C), §164.312(a)(1), §164.312(e)(1)**
6	Access to the physical facilities housing hosted systems is restricted to authorized users.	**CC 6.4** **HIPAA §164.310(a)(1), §164.310(a)(2)(i), §164.310(a)(2)(ii), §164.310(a)(2)(iii), §164.310(a)(2)(iv), §164.310(b), §164.310(c)**
7	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	**CC6.5** **HIPAA §164.310(d)(2)(i), §164.310(d)(2)(ii)**
8	Network security mechanisms restrict external access to the production environment to authorized ports and protocols.	**CC 6.6** **HIPAA §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(4)(i), §164.310(b)**
9	Connections to the production environment require encrypted communications.	**CC 6.6 and CC 6.7** **HIPAA §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(4)(i), §164.310(b), §164.312(e)(1)**
10	Antivirus or antimalware solutions detect or prevent unauthorized or malicious software on hosted systems.	**CC 6.8** **HIPAA §164.308(a)(5)(i), §164.308(a)(5)(ii)(B)**
11	System configuration changes are enforced, logged, and monitored.	**CC 6.8 and CC 7.1** **HIPAA §164.308(a)(5)(i), §164.308(a)(5)(ii)(B)**
12	Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution.	**CC 7.1** **HIPAA §164.308(a)(8), §164.312(a)(1), §164.312(c)(1), §164.312(c)(2), §164.312(e)(2)(i)**
13	System activities on hosted systems are logged, monitored, and evaluated for security events. Any identified incidents are contained, remediated, and communicated according to defined protocols.	**CC 7.2, CC 7.3, and CC7.4** **HIPAA §164.308(a)(1)(ii)(C), §164.308(a)(1)(ii)(D), §164.308(a)(6)(i), §164.308(a)(6)(ii), §164.314(a)(2)(i), §164.404(a)(2), §164.410(a)(1), §164.410(a)(2)**

	Complementary Subservice Organization Controls	Related Criteria
14	Access to make changes to hosted systems is restricted to appropriate personnel.	**CC 8.1**
15	Changes to hosted systems are documented, tested, and approved prior to migration to production.	**CC 8.1**

D. Complementary User Entity Controls

Nayya’s Platform was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Platform. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Nayya. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

	Complementary User Entity Controls	Related Criteria
1	Implementing controls to ensure only authorized individuals are granted access.	**CC 6.1, CC 6.2, and CC 6.3** **HIPAA §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(4)(i), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii) (C)**
2	Implementing controls to ensure access for terminated users is removed timely.	**CC 6.1, CC 6.2, and CC 6.3** **HIPAA §164.308(a)(3)(ii)(C)**
3	Implementing controls to ensure user accounts and access permissions are periodically reviewed.	**CC 6.2 and CC 6.3** **HIPAA §164.308a(1)(ii)(D), §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(3)(ii)(B), §164.308(a)(4)(ii)(C)**
4	Retaining ePHI data for six years from the date of its creation or the date when it last was in effect, whichever is later.	**HIPAA (§164.316(b)(2)(i)**

MOSSADAMS