Proprietary & Confidential

Glooko Core Platform

SOC 3

Relevant to Security, Availability, and Confidentiality

MAY 1, 2022 TO JULY 31, 2022

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Glooko AB and Glooko, Inc.
411 High Street
Palo Alto, CA 94301

To the Management of Glooko AB and Glooko, Inc.:

Scope

We have examined Glooko AB and Glooko, Inc.'s accompanying assertion in Section II titled "Glooko AB and Glooko, Inc.'s Assertion" (assertion) that the controls within Glooko AB and Glooko, Inc.'s Glooko Core Platform (system) were effective throughout the period May 1, 2022 to July 31, 2022, to provide reasonable assurance that Glooko AB and Glooko, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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*).

Glooko AB and Glooko, Inc. uses subservice organization Amazon Web Services (AWS) for hosting the production systems. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Glooko AB and Glooko, Inc., to achieve Glooko AB and Glooko, Inc.'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 Glooko AB and Glooko, Inc.'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 Glooko AB and Glooko, Inc., to achieve Glooko AB and Glooko, Inc.'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

Glooko AB and Glooko, Inc. 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 Glooko AB and Glooko, Inc.'s service commitments and system requirements were achieved. Glooko AB and Glooko, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Glooko AB and Glooko, Inc. 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 Glooko AB and Glooko, Inc.'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 Glooko AB and Glooko, Inc.'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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 Glooko AB and Glooko, Inc.'s Glooko Core Platform were effective throughout the period May 1, 2022 to July 31, 2022, to provide reasonable assurance that Glooko AB and Glooko, Inc.'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
October 24, 2022

II. Glooko AB and Glooko, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Glooko AB and Glooko, Inc.'s Glooko Core Platform (system) throughout the period May 1, 2022 to July 31, 2022 to provide reasonable assurance that Glooko AB and Glooko, Inc.'s service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Section III titled "Glooko AB and Glooko, Inc.'s Description of the Boundaries of Its Glooko Core 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 May 1, 2022 to July 31, 2022, to provide reasonable assurance that Glooko AB and Glooko, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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)*. Glooko AB and Glooko, Inc.'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 titled "Glooko AB and Glooko, Inc.'s Description of the Boundaries of Its Glooko Core Platform".

Glooko AB and Glooko, Inc. uses subservice organization Amazon Web Services (AWS) for hosting the production systems. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Glooko AB and Glooko, Inc., to achieve Glooko AB and Glooko, Inc.'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 Glooko AB and Glooko, Inc.'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 Glooko AB and Glooko, Inc., to achieve Glooko AB and Glooko, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Glooko AB and Glooko, Inc.'s complementary user entity controls assumed in the design of Glooko AB and Glooko, Inc.'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 May 1, 2022 to July 31, 2022, to provide reasonable assurance that Glooko AB and Glooko, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Glooko AB and Glooko, Inc.'s Description of the Boundaries of Its Glooko Core Platform

A. System Overview

1. Services Provided

Glooko AB and Glooko, Inc. (Glooko or the Company) was founded in 2010 to help patients track and manage their diabetes-related glucose and insulin dosage information using its mobile and web applications. In 2016, Glooko merged with Swedish company Diasend to enhance and build a more modern platform based on the strengths of each other's works in the blood glucose sector. The US headquarters are located in Palo Alto, California. The European headquarters are in Gothenburg, Sweden. Glooko currently employs over 175 people.

The Glooko Core Platform empowers the management of diabetes and other chronic conditions by collecting and unlocking the power of data from blood-glucose (BG) meters, continuous glucose monitors (CGMs), insulin pumps, connected insulin pens, wearables, connected scales, blood pressure cuffs, and activity trackers – bringing insights together in one place. Data is easily uploaded – remotely via app or in-clinic, securely shared, and visualized in actionable charts and graphs. This creates a solid foundation enabling collaboration and confident treatment decisions. The platform is compatible with over 95% of diabetes devices along with biometric devices, giving people with diabetes and chronic conditions and their care teams the freedom of choice.

The Glooko Core Platform's key functions are:

- Diabetes dosage, tracking, and management for consumers via the web portal and mobile application
- Diabetes treatment management for providers via the web portal
- Third-party partner integration for diabetes treatment and management via the Application Programming Interface (API)

2. Infrastructure

Glooko Core Platform utilizes AWS to host the application servers, database servers, and supporting services. Glooko uses US-East as its principal region for tasks and alternate regions for secondary and tertiary disaster recovery planning and replicated backups.

The web application is served through a redundant AWS Elastic Load Balancer connected to several AWS Elastic Compute Cloud (EC2) instances that host the app servers. The web application has a self-healing system that replaces non-responding AWS EC2 instances, which dynamically increase or decrease to provide minimal latency. These environments connect to several components, which complete the different operations required to process data from diabetes management devices. Once connected to the AWS Load Balancer through HTTPS/SSL, Glooko reaches one of the AWS EC2 instances in the VPC, which securely connects to the database to retrieve or add data. The data from diabetes management devices like BG meters, CGMs, and insulin pumps are uploaded to Glooko Core Platform by transmitters, uploaders, or mobile apps. The data is then parsed by Analyser, which then talks to the backend APIs and updates the data in the database. The data is then visualized in the web interface in the Summary, Logbook, Graphs, and Device settings. The clinician can generate a PDF report from the data and utilize the data in the web interface to manage the diabetes condition of their patients.

All the data transferred between the user's browser and Glooko's web servers, databases, and backend services is encrypted in transit on the database and at rest. Glooko uses SSL v1.2 and AES-256 encryption for transit.

3. Software

The Glooko Core Platform includes a web interface for health care professionals. It is written in a mix of Ruby on Rails, ReactJS, JavaScript, Node.js, RESTful API, and Python. The platform uses a Mongo database.

Configuration for interfaces is via simple tools intended for business users, IT analysts, or business analysts. Configuration for products, screens, workflows, and rules is handled through developer tools or a scripting language. Configuration for document authoring is handled via code.

Implementation is available through the Company's Delivery team or by a Systems Integrator (SI) partner. The Glooko Core Platform is deployed on AWS, and Glooko offers a SaaS delivery model that includes hosting, licenses, maintenance and support, upgrades of the license, and implementation of the upgrades.

The platform's configuration tools are designed to be used by non-IT staff. Customers are not allowed to touch core code. As a stand-alone solution, the Glooko Core Platform offers functionality, including support for dynamic forms attachment based on responses to customer data entry.

4. People

A Board of Directors is in place and oversees management activities. Reporting to the Board of Directors, the Chief Executive Officer (CEO) is responsible for the overall operation of Glooko. Glooko's senior management team reports directly to the CEO. In addition, Glooko has established a Security Working Board to oversee management's information security activities.

Reporting to the CEO, each member of the senior management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible, and a formal organization chart has been developed. The CEO is responsible for the overall operation of Glooko. Glooko's senior management, listed below, report directly to the CEO:

- Chief Operations Officer
- Chief Medical Officer
- Vice President, Quality & Regulatory Management
- Chief Technical Officer
- Chief Financial Officer
- Chief Commercial Officer

Glooko's organizational structure is reflective of its Glooko culture, nature, and scope of its operations. It also provides a framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. An interactive organizational chart is available for all employees on the Company's Human Resources (HR) system. The organizational chart presents the executive team, key areas of authority and responsibility, reporting relationships, and Glooko's overall organizational hierarchy. The executive team and other stakeholders of management review the reporting relationships and organizational structures on a periodic basis as part of organizational planning, as well as to respond timely to changing entity commitments and requirements.

5. Data

The Glooko Core Platform contains a variety of data, including PII. As directed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), PII is removed from all data that falls within the definition of Personal Health Information (PHI) before it is stored or exchanged. De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members. PHI includes:

- Name
- Address
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (date of birth, etc.)
- Telephone number
- Electronic mail address
- Social Security number
- Medical record number
- Device identifier and serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifiers

When confidential or sensitive information from one individual is received by another individual while conducting official business, Glooko requires users to set a password. Glooko does not reuse passwords or use simple passwords.

6. Processes and Procedures

Glooko's procedures are reviewed at least annually and updated as necessary to remain consistent with the system commitments and requirements.

Glooko's Code of Conduct, security, confidentiality, and disciplinary policies are communicated to employees upon hire. The policies are also available on an internal system for employees to reference, and any changes are communicated to employees via email. Additionally, with the acceptance of the employment offer, the employee acknowledges abiding by the policies communicated by HR.

Glooko's managed services and related support processes/procedures include but are not limited to:

- Onboarding procedures for new personnel and contractors to evaluate competency.
- Implementation support for new customers to ensure they have been provided with information on how to report failures, incidents, concerns, and other complaints to appropriate Glooko personnel.
- Access management procedures that ensure access to data, software, functions, and other IT resources are authorized, modified, or removed based on roles, responsibilities, or the system design.
- System development and maintenance procedures, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
- Change management procedures to ensure changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet Glooko's commitments and system requirements.
- Health and performance monitoring procedures to manage capacity demand and to enable the implementation of additional capacity to help meet Glooko availability commitments and system requirements.
- Incident response procedures that address incidents to ensure logical and physical security incidents, failures, and vulnerabilities are identified and reported to appropriate Glooko personnel and acted upon in a timely manner.
- Disaster recovery procedures that ensure environmental protection, software, data backup process, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet Glooko's commitments and system requirements.

B. Principal Service Commitments and System Requirements

Glooko provides customer access and use of its software subscription services as specified in the Master Services Agreement (MSA) and Software-as-a-Service (SaaS) Agreement. The overarching service commitment is to provide and secure Glooko's cloud-based enterprise software, designed for personalized remote patient monitoring for diabetes and other related conditions.

Glooko follows the principle of security to safeguard all protected information, which includes Personally Identifiable Information (PII), as well as the Glooko system as a whole. Glooko is committed to preventing unauthorized access and the potential abuse of information in order to meet contractual customer agreements, as well as statutory requirements. Glooko also maintains the service agreements and contracts with users and vendors to ensure that confidential information is not improperly disclosed.

In order to meet customer obligations, as well as abide by applicable laws and regulations for its services, Glooko is responsible for ensuring that the system is available to meet those requirements. With a commitment to availability in mind, Glooko maintains documented processes and employs redundancies as necessary to ensure that it meets its service level objective of system uptime. The Glooko identifies potential threats to the accessibility of the Glooko system and follows industry best practices to reduce the amount of downtime that would affect availability.

Glooko maintains confidentiality as it is required to ensure that the Company meets customer contractual obligations and applicable laws and regulations for information deemed confidential. Access to confidential data is limited to persons and users based on roles, needs, and permissions. Glooko's system logically protects data to prevent unauthorized access to its confidential data. The Company also maintains the service agreements and contracts with users and vendors in order to make sure that confidential information is not improperly disclosed.

Glooko's service commitments are documented in its contracts with customers. Among other items, they include:

- Security principles within the fundamental designs of the Glooko applications are designed to permit users access to the information they need based on their role as defined in the system while restricting them from accessing information not needed for their role. Roles are defined by each customer and are assigned a list of permissions accordingly.
- Glooko's service automatically locks up if left unattended for a specific period of time. Correct user credentials must be provided to re-access the application.
- Passwords are created by the customer and are required to be at least eight characters long and maintain a certain level of complexity. The password expiration term and reuse limit are configurable by the customer.
- The Glooko service communicates with secure Glooko-hosted and controlled servers and networks with the use of encryption technologies that protect user entities' information both in transit and at rest. Glooko disallows the use of low cipher strength in its Production service.
- Glooko ensures physical and technical security protections of customer data, as it uses servers located in highly secured hosting provider facilities that are subject to SOC 2 Type 2 examinations.

- Glooko employs redundant, next-generation firewalls, intrusion detection, and prevention services that are monitored twenty-four hours a day, seven days a week. Glooko uses internal and external threat prevention, delivering timely and accurate reports of its Production services.
- In addition to these controls, Glooko deploys up-to-date advanced threat protection services that help to identify, block, and track hacking attempts, scams, data breaches, adware, malware, spyware, trojans, phishing attempts, and other equally malicious requests.

Glooko system requirements are documented and communicated to employees through internal policies, standards, and procedures. These materials are available to all team members, and they agree to abide by them at the point of hire. The requirements include:

- System access is implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- System components are hardened consistent with internal standards.
- Confidential data are encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed and acknowledged by executive leadership.

Glooko's operational requirements that support the achievement of service commitments are communicated in its policies, procedures, and agreements with user entities. Glooko's policies and procedures define an organization-wide approach to how the system and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Glooko system.

C. Complementary Subservice Organization Controls

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

Complementary Subservice Organization Controls	
1	Hosted systems are scanned for vulnerabilities, and any identified vulnerabilities are tracked to resolution.
2	Anti-virus or anti-malware solutions detect or prevent unauthorized or malicious software on hosted systems.
3	Access to hosted systems requires strong authentication mechanisms.
4	Data at rest on hosted systems is stored in an encrypted format.

Complementary Subservice Organization Controls	
5	New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to being granted.
6	Terminated user access permissions to hosted systems are removed in a timely manner.
7	User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.
8	Privileged access to hosted systems and the underlying data is restricted to appropriate users.
9	Access to the physical facilities housing hosted systems is restricted to authorized users.
10	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
11	Network security mechanisms restrict external access to the Production environment to authorized ports and protocols.
12	Connections to the Production environment require encrypted communications.
13	System configuration changes are enforced, logged, and monitored.
14	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.
15	Access to make changes to hosted systems is restricted to appropriate personnel.
16	Changes to hosted systems are documented, tested, and approved prior to migration to Production.

D. Complementary User Entity Controls

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

This section describes additional controls that should be in operation at the user entities to complement the controls at Glooko. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	Alerting Glooko about any regulatory changes within their industry that might affect their services.
2	Allowing only authorized personnel to know and understand the services, networks, and supporting infrastructure of their Company.
3	Assisting Glooko with the identification and resolution of problems with the system as reasonable and required.

Complementary User Entity Controls	
4	Assuming responsibility for any loss or damage resulting from non-tested or inadequately tested procedures.
5	Describing changes such that Glooko can update documentation and monitor appropriately.
6	Ensuring that customers' employee access abilities are commensurate with the responsibility assigned to said employee.
7	Keeping usernames and passwords private.
8	Ensuring that customers are solely responsible for all use of their accounts and are prohibited from sharing passwords with third parties or attempting to access the system without providing a specifically assigned password.
9	Ensuring that customers are solely responsible for owning and managing their employees' access, including but not limited to removing any users' access who have been terminated, requiring a change in access, and terminating all access when the customer contract is terminated.
10	Providing a customer contact to authorize recovery services and verify data restoration.
11	Providing a list of all authorized personnel, vendors, or contractors that are allowed to provide support for their Company.
12	Providing recovery and back-out procedures to use in the event of change failure.
13	Responding in a timely fashion to requests for approving changes.
14	Ensuring that the customer transmits data to Glooko in a secure manner via SFTP or encrypted in password-protected files.
15	Ensuring that the customer is responsible for the accuracy and quality of data input by its users.
16	Approving configuration and user access rights per MSA and SaaS License Agreement.
17	Reviewing, approving, and authorizing Glooko to implement recommended problem resolution plans (if required).

MOSSADAMS