HIPAA Compliance for The Glooko Diabetes Management System

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to protect electronic data pertaining to patient identification and health, and standardize the process of data interchange. A major component of HIPAA is the “Security Rule”, which includes technical safeguards and their implementation. Technical safeguards are defined in 445 CFR Part 164 § 164.304:

*Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.*

The Security Rule's technical safeguards do not mandate a specific technology solution but rather employ the adaptable requirement that an entity use any and as many security measures as are reasonable and appropriate. These security measures are required to meet several standards, as described below. Glooko meets --and in many cases exceeds-- these standards while bringing innovative flexibility and features to the diabetes community of patients and providers.

**Access Control**

“Access” is defined in § 164.304:

*Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.*

The access control standard § 164.312(a)(1) requires that a covered entity must:

*Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).*

Access controls are designed to provide the appropriate privileges to users accessing data, applications and files. The HIPAA Security Rule describes implementation specifications for the access control standard:

**Unique user identification** § 164.312(a)(2)(i). *Assign a unique name and/or number for identifying and tracking user identity.* Glooko assigns each user a unique identification number, allowing it to route information appropriately and track user activity. Identity is established during registration by requiring the following fields: name, email address and password. In addition, provider organizations are required to give us a list of their verified staff members.

**Automatic logoff** § 164.312(a)(2)(iii). *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.* Patients of Glooko’s web service have to re-enter their password after 20 minutes of inactivity in order to continue using the service.
service. This is an added layer of security to protect the patients privacy from being displayed to others.

**Encryption and decryption** § 164.312(a)(2)(iv). Implement a mechanism to encrypt and decrypt electronic protected health information. To protect sensitive health information from unauthorized access, all data on the Glooko network is protected using the Secure Sockets Layer (SSL) protocol. In addition, Glooko forces the https:// standard for all mobile and web communication features, protecting from unauthorized access over wireless and wired networks. All data in the Glooko system is encrypted end-to-end using 256-bit Advance Encryption Standard (AES) encryption for message data both in motion and at rest.

**Audit Control**

The audit control standard § 164.312(b) requires that a covered entity must:

> Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Glooko records and examines network activity to protect users, technical infrastructure and electronic health information from security violations.

**Integrity**

“Integrity” is defined in § 164.304:

> Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

The integrity standard § 164.312(c)(1) requires that a covered entity must:

> Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Glooko protects the integrity of electronic health information on its secure platform via end-to-end encryption and decryption of messages transferred over the SSL protocol. To protect against destruction, all data is securely archived on a central server after encryption.

**Person or Entity Authentication**

The person or entity authentication control standard § 164.312(d) requires that a covered entity must:
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

To verify identity upon website access or mobile installation, Glooko authenticates with either login or registration. Existing user login requires a username and password. During registration, identity is established by requiring the following fields: name, email address and password. Providers are identified and authenticated by the organization to which they belong.

Protected Health Information – Data Storage

Glooko leverages a cloud-based platform to store PHI (protected health information). Technology partners used to create and maintain this platform are business associates as defined at § 160.103. As a covered entity, Glooko has signed contracts with business associates requiring them to comply with the HIPAA requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, Glooko’s business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

Transmission Security

The transmission security standard § 164.312(e)(1) requires that a covered entity must:

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

There are two implementation specifications for the transmission security standard:

Integrity controls § 164.312(e)(2)(i). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Encryption § 164.312(e)(2)(ii). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Glooko’s Secure Socket Layer (SSL) Handshake Protocol uses a 256-bit Advance Encryption Standard (AES) encryption for data both in motion and at rest. This cryptosystem forces the secure https:// standard for all mobile and web access to communication features, protecting the data from unauthorized access over wireless and wired networks.

Summary:

Today, people with diabetes and their providers face many challenges in the way they manage the disease. Information about blood glucose levels, insulin, carbohydrates, and exercise is being stored in numerous places like multiple BG (blood glucose) meters,
pumps, CGMs, log books, and diaries making it difficult to access or trust the accuracy of the data.

Glooko offers a diabetes management system that is agnostic of diabetes device manufactures. Once the patient syncs their health data to the Glooko platform, it can be accessed from any web browser, or the Glooko mobile applications. Patients can also grant access to a provider or group of providers, enabling them to access the health data from any web browser, or Glooko mobile applications.

**Highlights of Glooko’s Security and Compliance Components**

- User Identification and Verification
- Authentication to Confirm the User’s Identity
- SSL Handshake Protocol with AES
- Encrypting all Data in Motion or at Rest
- Automatic Log-off During Inactivity
- Audit Control to Protect Users from Security Violations
- Backup of All Network Activity

Glooko is a free application that can be utilized on iPhone, Android and the web. HIPAA compliance and data security is a top priority for Glooko’s communication platform. We welcome any additional questions, ideas or feedback at support@glooko.com.