Diabetes Remote Patient Monitoring and HIPAA Compliance

May 2016

Background

Since the Affordable Care Act passed into law, more and more healthcare organizations are moving towards “at-risk” payment, as evidenced by the growth of Accountable Care Organizations (ACOs). At-risk payment reimburses the health system a pre-set amount per patient, whether the patient uses the services or not, and allows the health system to share in any savings. By emphasizing and rewarding preventative care, patients with chronic conditions, like diabetes, could be less likely to need costly services resulting from complications. Patients benefit by staying healthier over a longer period of time and the health system benefits by being able to keep a greater margin per patient.

For at-risk health systems, remote patient monitoring can be a powerful tool to help patients better manage their conditions and reduce the use of expensive services such as emergency room visits or hospital admissions. Diabetes is a condition that is well suited for remote patient monitoring. Blood glucose values are impacted by a wide array of factors including medication, food, activity levels, hormones and stress – these factors can be in a constant state of flux, making managing blood glucose levels extremely challenging. With remote patient monitoring, healthcare providers can provide patients with timely insight and support to help decipher blood glucose trends and identify the appropriate course of action to improve. Through automation and on-demand data sharing, this process can be easy and convenient for both the care team and the patient. When sharing health data, security and controls is paramount. This paper discusses the value of remote patient monitoring and the importance of keeping data secure when providing remote care. It specifically covers Glooko’s HIPAA compliance components.
Glooko: A Diabetes Remote Patient Monitoring Solution

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 stored in disparate places like multiple blood glucose (BG) meters, insulin pumps, continuous glucose monitors (CGMs), log books and diaries, making it difficult to access or trust the accuracy of the data.

Glooko is a diabetes management platform that enables patients and their healthcare team to see all their diabetes data in a central location. Glooko is a device agnostic solution and is compatible with the majority of diabetes devices on the market—patients can sync their diabetes data to Glooko from 40+ meters, pumps and CGMs. Once the patient syncs their health data to the Glooko platform, it can be securely accessed from any web browser via the Glooko Web App or via the Glooko Mobile App. Patients can also grant access to a provider or group of providers, enabling them to securely access the health data from any web browser to provide remote support.

HIPAA Considerations for Remote Patient Monitoring Solutions

While remote patient monitoring can provide great benefits to both patients and health systems, solutions must ensure they protect patient information and adhere to the guidelines of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

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.

Passwords Glooko goes beyond the published HIPAA rules to ensure that passwords are secure. With Glooko passwords must be at least eight (8) characters in length, must not use control characters and other non-printing characters, and must contain characters from at least three of the following four categories arranged in any order.

• English uppercase characters (A through Z)
• English lowercase characters (a through z)
• Base 10 digits (0 through 9)
• Non-alphabetic characters: ~!#$%^&*;?.+_
password after 20 minutes of inactivity in order to continue using the application. This is an added layer of security to protect 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 protected health information (PHI). 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**

The evolution in payment models and the pure value of providing care in between doctor visits have encouraged the implementation of remote patient monitoring programs, which can greatly benefit both patients and health systems by providing more timely care and reducing use of costly services. To operate safely and securely, remote patient monitoring solutions must ensure they are HIPAA compliant and protect patient information. Glooko is a remote patient monitoring solution for diabetes that meets HIPAA standards, enabling patients and their care teams to more seamlessly manage the complex condition of diabetes while protecting patient privacy.

**About Glooko**

Glooko is the world’s leading Unified Platform for Diabetes Management and is trusted by the world’s leaders in diabetes care. Glooko provides an FDA-cleared, HIPAA-compliant Web and Mobile application designed to improve health outcomes for people with diabetes, which in turn reduces costs for payers and the healthcare system. Glooko seamlessly syncs with over 40 blood glucose meters and major fitness and activity trackers and supplies timely, verified patient data such as blood glucose, carbs, insulin, blood pressure, diet and weight data. Glooko’s mobile app enables patients to easily track and proactively manage all aspects of their diabetes care. Glooko’s population management web app and API’s offer diabetes-centric analytics and supplies insightful reports, graphs and risk flags to health systems and payers. Learn more at www.glooko.com and follow us at Twitter.com/GlookoInc and Facebook.com/Glooko.