Focused Future, LLC
E-QPASS HIPAA Safety and Security Statement
_____

Overview

The purpose of this statement is to document and describe the fact that both Focused Future, LLC ("Vendor") and MAD Technology Solutions, LLC ("Developer") adhere to a high level of standards and best practices to ensure that the E-QPASS product and services ("QPASS") are safe and secure and meet HIPAA standards.

Administration and Privacy

Vendor, as the owner of the copyrighted product, retains the rights to the collected data via the proprietary product. Vendor does not store data outside of this secure application.

The developer has gone through a complete auditing process to ensure that its company is verified as HIPAA compliant. Using Compliancy Group, Developer has submitted not only its business operations, policies and procedures but also its software development life cycle practices and all comply with and have been verified as compliant with HIPAA. Please see the attached Seal of Compliance and matching certificate.

Data Safety and Security

Building upon the HIPAA verification defined above, Developer also uses best of breed partners to manage and maintain both the online operations and data management of e-QPASS. This includes the Microsoft Azure Cloud services platform and the Microsoft .NET family of products.

e-QPASS uses a dedicated server hosted within the Microsoft Azure environment. This environment itself has been certified as SOC Type II compliant and meets or exceeds all other types of industry compliance concerns.

e-QPASS sits behind a Microsoft Network Security Group (software firewall) that allows only the required traffic through the dedicated server. This would include external management and maintenance of the server by Developer staff using Trusted Locations and HTTPS for web application traffic used by end users of e-QPASS.

e-QPASS further ensures the safety, security and integrity of its data by using encrypted disk drives on the dedicated server. This is enabled by default and cannot be disabled at any time.

e-QPASS also uses additional encryption techniques for PII and other data classified as sensitive. This follows both industry best practices as well as accepted design patterns regarding database design and administration for both Microsoft environment and other DBA environments in general.

e-QPASS ensures that all transmission of data is secure using the highest available levels of encryption protocols and uses SSL certificates issued by reputable certificate authorities. HTTPS is the only protocol allowed through the firewall and the web server itself further enforces that all traffic flows under secure protocols. All other outbound traffic that does not travel under secure protocols (such as notification emails and management reports) is blinded and striped of all individually identifiable data and primarily used in an aggregate basis.

NOTE: All reports that are specific to the Client ("Patient") are also blinded but is ultimately under the control and responsibility of the Covered Entity ("End User").

QPASS is protected through a complete backup and disaster recovery program that includes intra-day data snap shots of the database to disk and daily offsite backups of the database to a secure data center. This database too is SOC Type II compliant.

Contact:

Focused Future, LLC

Email: FocusedFuture@gmail.com

MAD Technology Solutions, LLC

MDrawbaugh@justgetmad.com

December 2020

HIPAA Seal of Compliance Certificate

By utilizing Compliancy Group's Achieve, Illustrate, Maintain (AIM) methodology,
MAD Technology Solutions, LLC *has completed the implementation of its HIPAA compliance program and has been presented the HIPAA Seal of Compliance as means of verification.*

AUTHORIZED BY :   COMPLIANCY GROUP

SIGNATURE: *Marc Haskelson*

President & CEO