Pariox LLC Security Policy
(HIPAA Compliance Statement)

This Policy identifies and describes the HIPAA compliant security measures we have in place to protect the data that is transferred and stored on Pariox and our Server.

Secure Software-User Identifiers.

All Passwords are encrypted with the MD5 (Message-Digest algorithm 5) cryptographic hash function. Passwords created by Users must meet strength restrictions in order to be valid. The strength restrictions make sure that each Password is complex, containing at least 8 characters, at least one capital letter, one lowercase letter and one number. In addition, all Passwords expire every 90 days. Upon renewing their Password Users cannot use a Password they have used within the last 180 days. Passwords created by Pariox or our IT employees expire immediately and must be renewed upon the User's next login before the User can continue navigating through Pariox.

Secure Socket Layer Encryption.

All data that is stored on our server, transmitted to our server or that we transmit to Users during their logon session is encrypted using 256-bit Secure Socket Layer encryption. In addition, we encrypt all individually identifiable health and financial information.

Secure Server.

Hardware firewalls, vulnerability scans, and antivirus software protect our data and dedicated Server from malicious and unauthorized access to the information contained within Pariox. Our dedicated Server, network devices and backup data storage media are housed in a SAS70 Type II Certified facility. On-site video monitoring and military-grade validation systems secure the perimeters of the data center and prevent unauthorized entry.

Pariox Activity Review.

We have automated auditing tools and techniques in place that log information such as:

-Which User accessed Pariox; what time the User accessed Pariox; what data was accessed during the User's logon session
-IP address
-Cookie ID (Session ID)

Access Management.

Pariox team members (our employees, agents, and subcontractors) are granted access to our secure server and database only as needed to perform their legitimate job functions—to maintain, restore and develop Pariox. Our team members are required to agree to and sign our Confidentiality Agreement, Privacy Policy, Acceptable Use Policy and undergo yearly HIPAA Privacy and Security Awareness training.

Contingency Plan.

Data back ups are performed to ensure we have an exact replica of the data stored on our Server. These Data backups play a key role in our Disaster Recovery and Emergency Mode Procedures.

General Notices.

Each User's efforts to protect against unauthorized access play an important role in protecting the security of sensitive data stored and transferred on Pariox and our Server.

Pariox may have links to other, outside web sites that we do not control. We are not responsible for the content or privacy policies of these sites, and Users should check those policies on such sites.

If you believe there has been a security breach of any kind, please contact our Chief Security Officer immediately at security@pariox.com

Pariox LLC reserves the right to change this Policy at any time. Any such modifications will be automatically and immediately effective. We are not responsible for informing Clients and Users directly of any modifications to this Policy. Clients and Users should regularly review this Policy available on our website: www.pariox.com