Pariox LLC Privacy Policy

Pariox LLC ("we", "us", "our") provides web-based software applications, services and other products on the Pariox web site (here in after collectively referred to as "the Software") to home healthcare agencies, staffing agencies and healthcare professionals (here in after "Client", "your employer") and their employees, sub-contractors and agents ("user(s)", "you", "your"). This Policy identifies and describes the way we use and protect the information we collect about you.

Information about You

In order to use and have access to the Software you need to set up a User account, a process that must be authorized by a Client of Pariox LLC (most commonly your employer). Certain information is required to set up a User account such as your name and email address. Once you are an authorized User, other information can be entered either by yourself, your employer(s) or other authorized entity(s) that authorized you to access the Software. Such 'other' information may include HR documents and financial information (pay rates and/or credit card information if you are a Client of the Software).

Who can access your information?

Only you and the authorized entity(s) that granted you access to the Software can view, edit, delete and add personal information to your User profile such as payment rates, address, phone numbers, and personnel files which may include but are not limited to: CPR card, driver's license, physical statement, professional license, and auto insurance.
'Shared' information does NOT include your Password, USER ID and E-Signature, which you must keep confidential at all times.

What do we do with the information we gather?

All information that is transmitted to the Pariox servers or that we transmit to authorized users during their logon session is encrypted using 256-bit Secure Socket Layer encryption. In addition, we de-identify (encrypt) SSNs and passwords with a "second layer" of encryption directly in the MySQL database.

Our 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 the Software. 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.

We never sell personal information to third parties that could be used to specifically identify an individual User. Anonymous data is sometimes shared with third parties. We do provide personal information to government agencies as required by law or regulation, and in connection with investigations of possible illegality or misuse of Pariox LLC products and/or services.

We may disclose personal information if we are required to do so by law or we in good faith believe that such action is necessary to (1) comply with the law or with legal process; (2) protect and defend our rights and property; (3) protect against misuse or unauthorized use of the Software; or (4) protect the personal safety or property of our Users or the public (among other

things, this means that if you provide false information or attempt to pose as someone else, information about you may be disclosed as part of any investigation into your actions).

What steps do we take to keep your information secure?

We store the information you provide to the Software on our secure Servers. These Server are protected from malicious and unauthorized access by hardware firewalls, vulnerability scans, and antivirus software. In addition, all information that is stored on our server, transmitted to our server or that we transmit to our Users during their logon session is encrypted using 256-bit Secure Socket Layer encryption. Passwords are also encrypted using the MD-5 cryptographic hash function.

To further protect against unauthorized use of the Software, we have implemented automated tools and techniques that log information about your use of the Software. Information collected during a logon session includes (but is not limited to):

-What and when a user accessed a patient's file in the system
-These specific user activities are logged: Assignment deleted, created assignment, deleted treatment, Patient profile edited, View Patient Record, SOC created, Visit Created, Visit Deleted, and Visit Edited

What steps can you take to keep your information secure?

Your own efforts to protect against unauthorized access play an important role in protecting the security of your personal information and patient information. You should be sure to LOG OUT of the Software at the end of each logon session, and go 1 step further by logging out of the browser used to access the Software.

We 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.

Do we do Surveys?

From time to time, we may ask you to fill out a survey on the Pariox website to help us better understand our Clients' and Users' needs. You may opt-out of participating in such surveys. We will not disclose survey response information to any other party and will solely use surveys internally.

What are my choices?

You may choose to delete, edit or add information to your User account at any time.

You may choose to discontinue use of the Software at any time. After termination of your User account we will continue to treat and protect your personal information in accordance with this Policy.

Children.

Our services are not directed to persons under the age of 18. And we do not knowingly collect information from persons under the age of 18.

Risks inherent in sharing information.

Although by having a User account your personal information is only shared between you and the entity that grants you access to the Software, you must be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you share your information, including your employer or other authorized entity—we cannot guarantee that only authorized persons will view your information. We are not responsible for third party circumvention of any privacy settings or security measures on the Software. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software (including firewalls).

When accessing our Software you may be introduced to, or be able to access or link to certain third-party websites or advertisements created or hosted by third-party advertising companies. We may analyze the personal information you provide us and use that information to display the links, web sites, and advertisements we believe may be of relevance to you.

Patient Information

Through the Software, authorized Users can access, modify, transmit, store, create and upload electronic medical records and other confidential data pertaining to patients and Users including but not limited to individually identifiable health information, financial information, and personnel files. We protect all individually identifiable health and financial information of patients and Users in accordance with the Software License Agreement between our Clients and us.

Privacy Contact Information

We value your opinions. If you have any questions, concerns, or comments regarding our Privacy Policy, please contact our Chief Security Officer at security@pariox.com.

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