Privacy Policy for PSPN Veteran's Administration Clinicians and Administrative Personnel

Last updated: 08/23/2023

---

1. Introduction

Welcome to the Primary Spine Provider Network (PSPN)! As a healthcare organization, we are dedicated to ensuring the privacy and security of personal and sensitive information, including the data shared with the Veteran's Administration (VA) for the purposes of clinician satisfaction, training, engagement, and educational content evaluation. This Privacy Policy outlines how we collect, use, share, and protect the information of our clinicians and administrative personnel while collaborating with the VA. By participating in our initiatives, you agree to the practices described in this policy.

---

2. Information We Collect

We collect various types of information for the purpose of clinician support, ascertaining clinician beliefs, empowering care delivery, and enhancing clinician experience, including:

- Personal Information: This includes your name, contact details, professional credentials, and other information necessary for employment and credentialing and/or participation.
- Health Information: In the course of providing healthcare services training and support, although unlikely, we may collect and process patient health information (protected health information or PHI) in accordance with applicable laws, such as the Health Insurance Portability and Accountability Act (HIPAA). You will be notified if and when this type of data is collected.
- Administrative Data: We collect data related to your employment or affiliation with the VA, along with your usage of the PSPN platform including PSPN administrative communications and queries from you to PSPN support staff.
- Training and Engagement Data: We may collect information about training completion, clinician engagement, and tool/utility usage, downloads and clinician surveys.

---

3. How We Use and Share Your Information

We may use and share the collected information for the following purposes:

- Employment and Credentialing: We may use your information to manage your employment relationship, including onboarding, benefits administration, and maintaining professional credentials.
- Healthcare Services: For clinicians, we use health information to help you provide patient care, maintain medical records, and ensure compliance with healthcare standards and regulations.
- Clinician Satisfaction and Engagement: We share de-identified and aggregated data with the VA to assess clinician satisfaction, beliefs, and engagement. This data sharing supports ongoing improvement in the work environment and enhances the quality of care provided.
- Training and Educational Content Evaluation: We may share data related to training completion and educational content uptake with the VA to evaluate the effectiveness of training programs and educational materials.
- Content Consistency: We may share information regarding content consistency with the best available evidence to ensure alignment with clinical guidelines and best practices.

---

4. Data Security

We understand the critical importance of safeguarding the confidentiality and integrity of the information we collect and process. As a healthcare organization collaborating with the Veteran's Administration (VA), we have implemented stringent security measures to ensure that your personal and sensitive information remains protected. Our commitment to data security encompasses technical, administrative, and physical safeguards, including:

- Administrative Safeguards: Access to your information is strictly controlled on a need-to-know basis. Our personnel undergo comprehensive training on data privacy and security protocols to ensure they understand the importance of handling sensitive information responsibly. We maintain detailed access logs and conduct regular audits to monitor and restrict unauthorized access attempts.
- Technical Safeguards:
    - Firewalls: We employ firewalls to create a protective barrier between our internal network and external threats. Firewalls are configured to allow authorized communication while blocking unauthorized access attempts.
    - Intrusion Detection and Prevention Systems (IDPS): Our systems are equipped with IDPS that actively monitor network traffic for suspicious activity or unauthorized attempts to access our platform. These systems can automatically respond to and block potential threats.
    - Multi-factor Authentication (MFA): We implement MFA to add an extra layer of security to administrator accounts. This requires administrators to provide two or more forms of authentication before gaining access, reducing the risk of unauthorized access due to compromised credentials.
    - Regular Security Assessments: Our platform undergoes regular security assessments, including vulnerability scanning and penetration testing. This proactive approach helps us identify and address potential vulnerabilities before they can be exploited by malicious actors.

- Encryption Techniques:
    - Transport Layer Security (TLS): We utilize TLS encryption to secure data transmitted between your device and our servers. This encryption ensures that data remains confidential during transit and guards against eavesdropping or data interception.
    - Data Encryption at Rest: Personal and sensitive information stored on our servers is encrypted at rest. This means that even if someone gains access to our servers, the data remains encrypted and unreadable without the appropriate decryption keys.
    - End-to-End Encryption: In certain cases, such as communication between users, we implement end-to-end encryption. This means that only the intended recipients can decipher the information exchanged, ensuring that even if intercepted, the data remains confidential.
    - Strong Cryptographic Algorithms: Our encryption techniques are based on industry-standard cryptographic algorithms that have been proven to provide robust security. These algorithms are regularly reviewed and updated to ensure that we stay ahead of emerging threats.
- Cloud Security: To enhance the security of your information, we rely on cloud infrastructure provided by industry-leading server and vendor partners. These partners are recognized for their commitment to maintaining the highest standards of security and data protection. Our cloud services are hosted on servers and platforms that adhere to industry best practices, employing robust security features such as multi-factor authentication, data encryption at rest, and continuous monitoring.

While no system can guarantee absolute security, we are committed to employing a multi-layered approach to protect your data and maintain your trust. If you have any questions or concerns about our data security practices, please don't hesitate to reach out to our Privacy Officer at [contact email address].

---

5. Your Rights

You have rights concerning your information:

- Access: You can request access to your personal and health information that we hold.
- Correction: You can request corrections to inaccuracies in your information.
- Withdrawal: You can withdraw consent to process certain information, where applicable.

---

6. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. We will notify you of any significant changes and obtain your consent if required by applicable laws.

7. Contact Us

For questions, concerns, or requests related to your privacy, please contact our Privacy Officer at info@primaryspineprovider.com.