Privacy Policy for BotOn Health (HIPAA & GDPR Compliant)

At BotOn Health, we prioritize the privacy and security of your personal and health-related information. This Privacy Policy explains how we collect, use, and protect your data in compliance with the **Health Insurance Portability and Accountability Act (HIPAA)**, the **General Data Protection Regulation (GDPR)**, and other applicable privacy laws.

1. Information We Collect

We may collect the following types of information:

- **Personal Identifiable Information (PII)**: Such as name, email address, phone number, and other contact details.
- **Protected Health Information (PHI)**: Health-related information that may include medical history, treatment data, and any other details that qualify as PHI under HIPAA.
- **GDPR-Regulated Personal Data**: For EU users, any personal information (such as IP address, location data, or online identifiers) that is subject to the GDPR.
- **Usage Data**: Information about how you interact with our website and services, including IP address, browser type, and device information.
- **Cookies**: We use cookies and similar technologies to enhance user experience and track website performance. You can manage your cookie preferences through your browser settings.

2. How We Use Your Information

We use the data we collect, including your **PHI** and personal data, for the following purposes:

- **Healthcare Services**: To deliver health-related services, such as managing appointments, coordinating care, and providing treatment or advice.
- **Communication**: To send service updates, appointment reminders, or respond to inquiries.
- **Operational Efficiency**: To manage billing, handle insurance claims, and ensure efficient service delivery.
- **Analytics**: To analyze and improve the performance of our website and services.
- **Legal Compliance**: To comply with HIPAA, GDPR, and other applicable legal and regulatory obligations.

3. Legal Basis for Processing Under GDPR

For users in the European Union, we process your personal data based on the following legal grounds:

- **Consent**: Where you have given explicit consent for us to process your data.
- **Contract**: Where processing is necessary for the performance of a contract, such as providing healthcare services.
- **Legitimate Interest**: For purposes like improving our services, provided that your rights are not overridden.
- **Legal Obligations**: To comply with legal requirements, such as healthcare regulations under HIPAA.

4. How We Share Your Information

We do not sell or rent your personal information. However, we may share your data in the following cases:

- **Healthcare Providers**: With other healthcare providers involved in your care, as allowed under HIPAA.
- **Business Associates**: With third-party vendors or service providers, ensuring that they comply with HIPAA and GDPR requirements.
- **Legal Requirements**: When required by law, such as in response to a legal request or to protect the health and safety of individuals.
- **International Transfers**: If your data is transferred outside of the European Economic Area (EEA), we ensure that the transfer is legally compliant (e.g., through the use of Standard Contractual Clauses).

5. HIPAA & GDPR Security Measures

We employ strong security protocols to protect your **PHI** and personal data:

- **Encryption**: All sensitive data is encrypted in transit and at rest to prevent unauthorized access.
- **Access Control**: We limit access to your data to authorized personnel only.
- **Audit Logs**: We maintain audit trails for any access to **PHI**, in compliance with HIPAA.
- **GDPR Data Protection Impact Assessment (DPIA)**: We conduct DPIAs where necessary to ensure compliance with GDPR.
- **Security Awareness Training**: Our staff receives regular training on both HIPAA and GDPR regulations to ensure full compliance.

6. Your Rights Under GDPR and HIPAA

Depending on your location, you have several rights regarding your data:

Under GDPR (for EU users):

- **Right to Access**: You can request a copy of the personal data we hold about you.
- **Right to Rectification**: You can request corrections to any inaccurate or incomplete data.
- **Right to Erasure**: You can request the deletion of your personal data under certain circumstances.
- **Right to Restrict Processing**: You can request that we limit how we process your data.
- **Right to Data Portability**: You have the right to request the transfer of your data to another organization or to yourself.
- **Right to Object**: You can object to certain types of data processing, including direct marketing.
- **Right to Withdraw Consent**: You can withdraw your consent at any time, where processing is based on consent.

Under HIPAA (for U.S. users):

- **Right to Access**: You have the right to request access to your PHI.
- **Right to Amend**: You may request corrections to your PHI.
- **Right to an Accounting of Disclosures**: You can request a record of how your PHI has been shared.
- **Right to Request Restrictions**: You can request limitations on the use or sharing of your PHI, although we may not always be able to accommodate these requests.

To exercise any of these rights, please contact us at [kdiaz@botondesk.com].

7. Data Retention

We retain your personal data and PHI only for as long as necessary to fulfill the purposes described in this policy or as required by law. After this period, we will securely delete or anonymize your data in compliance with both **HIPAA** and **GDPR** requirements.

8. Breach Notification

In compliance with both **HIPAA** and **GDPR**, we are required to notify you and relevant authorities in the event of a data breach involving your personal information or PHI. We will take immediate steps to mitigate any harm and prevent future breaches.

9. Data Transfers and International Transfers

For **GDPR** compliance, if your personal data is transferred outside of the European Economic Area (EEA), we ensure that adequate safeguards are in place, such as **Standard Contractual Clauses** or other lawful mechanisms.

For **HIPAA** compliance, all data is handled according to strict privacy and security rules to protect **PHI** within the United States.

10. Children's Privacy

Our services are not intended for individuals under the age of 13, and we do not knowingly collect or store information from children under this age. If we become aware that we have inadvertently collected data from a child, we will promptly delete the information in compliance with applicable laws.

11. Updates to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, regulatory requirements, or legal obligations. Any updates will be posted on this page with a revised "Last Updated" date.

12. Contact Information

For any questions regarding this Privacy Policy, or to exercise your privacy rights, please contact us at:

BotOn Health
Email: kdiaz@botondesk.com
Phone: +1 6782607976
Address: 207 15th ST NE. Atlanta, GA.

For GDPR-specific concerns, you may also contact our **Data Protection Officer (DPO)** at **soporte@dynamosmartsolutions.cl**

Last Updated: 10/18/2024