HIPAA Compliance Policy Regarding Protected Health Information (PHI) in Connection with Continuous Glucose Monitoring (CGM) Devices, Insulin Pumps, & Additional Supplies
Effective Date: 2/24/2025

Serra Diabetics

Introduction

Serra Diabetics LLC dba Serra Diabetics ("Serra Diabetics") recognizes its legal and ethical obligation to protect the confidentiality, integrity, and availability of all Protected Health Information ("PHI") it handles in the course of its operations. In compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Privacy, Security, and Breach Notification Rules codified at 45 CFR Parts 160 and 164, Serra Diabetics has established this policy to govern its collection, use, disclosure, storage, and protection of PHI associated with continuous glucose monitoring ("CGM") devices, insulin pumps, and additional supplies. This policy reflects Serra Diabetics' ongoing commitment to maintaining robust data protection practices in accordance with applicable federal regulations.

Scope of Policy

This policy applies to all business units, personnel, processes, and third-party relationships through which Serra Diabetics creates, receives, maintains, or transmits PHI in connection with CGM monitors, insulin pumps, and additional supplies or services. This includes, but is not limited to, interactions with consumers via the website, data-sharing arrangements with business associates, and internal handling of sensitive health information. We may update this HIPAA Policy periodically to reflect changes in our practices, technologies, or legal requirements. Material changes will be communicated as required by law and posted on our website with an updated effective date. Continued use of our services after changes constitutes acceptance of the updated policy. We encourage you to review this HIPAA Policy periodically to stay informed about how we are protecting your privacy.

Policy Provisions

1. Limitation on PHI Collection

Serra Diabetics carefully limits PHI use to what is essential for care and operations, consistently upholding and exceeding HIPAA's "Minimum Necessary" standard. PHI is collected strictly to the extent required to fulfill product orders, deliver related services, and support patient health management involving CGM devices, insulin pumps, and additional supplies. This may include identifiers, health status, medical histories, and treatment data necessary for facilitating accurate and lawful fulfillment of orders.

2. Data Storage and Security Protocols

All PHI maintained by Serra Diabetics is stored in encrypted systems utilizing protocols that meet or exceed current industry standards for cybersecurity, including but not limited to AES-256 encryption during both storage and transmission. Access to these systems is physically and electronically restricted to authorized individuals only. Comprehensive administrative, technical, and physical safeguards are in place to ensure PHI remains secure at all times.

3. Role-Based Access and Authentication Controls

Only individuals whose job responsibilities require access to PHI may be granted such access. User access is governed by a strict authentication process involving unique user identifiers, password controls, and role-based privileges. Serra Diabetics maintains audit logs to monitor access and detect unauthorized attempts in real time.

4. Workforce Training and Awareness

All employees, agents, and contractors who may come into contact with PHI are subject to mandatory HIPAA compliance training upon hire and at regular intervals thereafter. Training covers legal obligations, internal procedures, and best practices regarding data protection, ensuring all workforce members understand and are accountable for safeguarding PHI.

5. Business Associate Agreements (BAAs)

All external entities engaged by Serra Diabetics that may encounter PHI such as payment processors, shipping providers, or data hosting services must enter into a legally binding Business Associate Agreement (BAA) with Serra Diabetics. These agreements contractually obligate third parties to adhere to all applicable HIPAA standards and provide satisfactory assurances of their compliance.

6. Breach Detection and Notification Procedures

In accordance with the HIPAA Breach Notification Rule, Serra Diabetics maintains a comprehensive incident response protocol to address suspected or confirmed breaches of PHI. This includes immediate containment, investigation, risk assessment, and, when applicable, timely notification to affected individuals and the U.S. Department of Health and Human

Services (HHS). Notification shall be provided without unreasonable delay and no later than 60 calendar days after discovery of a breach, consistent with 45 CFR §164.404.

7. Risk Management and Assessments

Serra Diabetics conducts regular and systematic risk assessments to evaluate the effectiveness of security controls, identify vulnerabilities, and update practices in response to technological developments or regulatory changes. Risk assessments are documented and reviewed by senior management as part of Serra Diabetics' continuous improvement strategy.

8. Appointment of HIPAA Privacy and Security Officer

Serra Diabetics has appointed a designated HIPAA Compliance Officer who bears primary responsibility for overseeing the implementation, maintenance, and enforcement of this policy. The Compliance Officer serves as the point of contact for HIPAA inquiries, complaints, and compliance audits. Questions may be directed to the Officer at: regulatory@serradiabetics.com.

9. Individual Rights under HIPAA

In accordance with 45 CFR §164.524 and §164.526, individuals whose PHI is maintained by Serra Diabetics are entitled to exercise certain rights, including the right to access their records, request corrections or amendments, and obtain an accounting of disclosures made by Serra Diabetics. Requests may be submitted through secure, authenticated channels provided by Serra Diabetics, and will be processed in a timely manner in accordance with HIPAA timeframes.

Conclusion

This policy reaffirms Serra Diabetics' unwavering commitment to ensuring the privacy and security of all PHI entrusted to it in connection with CGM devices, insulin pumps and supplies, and related services. Serra Diabetics continuously monitors developments in applicable law and industry standards, and shall revise this policy as necessary to maintain full compliance with HIPAA and to preserve the trust of its patients, customers, and partners.