Data Privacy, Sharing with Third-Party Software Providers, and Cybersecurity

The Dr. Bawani Marsden Clinic is committed to safeguarding the privacy and security of patient information. In the course of providing medical services, the clinic may utilize third-party software providers for purposes such as appointment scheduling, billing, electronic medical record management, and telehealth services. The clinic ensures that any third-party providers involved in handling patient data are in compliance with relevant privacy laws and adhere to robust cybersecurity practices to protect patient data.

1. Purpose of Data Sharing

Patient information may be shared with third-party software providers for the following purposes:

- To schedule and manage appointments
- To process billing and payments
- To maintain and update electronic medical records
- To facilitate telehealth consultations
- To ensure the smooth operation and delivery of services provided by the clinic

2. Types of Data Shared

The types of patient data that may be shared with third-party software providers include:

- Personal identification information (e.g., name, address, date of birth, contact details)
- Medical history and treatment records
- Appointment information, including dates, times, and any special requirements
- Billing and payment details, including insurance information, if applicable

3. Data Security and Cybersecurity Measures

The clinic recognizes the critical importance of protecting patient data from unauthorized access, alteration, or disclosure. As such, both the clinic and its third-party software providers implement robust cybersecurity measures to secure patient data. These measures include:

- **Encryption**: All patient data, including sensitive information such as medical records, is encrypted during storage and transmission to ensure it is protected from unauthorized access.

- **Access Control**: Only authorized personnel and healthcare providers with legitimate purposes have access to patient data. Access controls, including secure passwords and multi-factor authentication, are implemented to protect patient data from unauthorized users.
- **Regular Audits**: The clinic and its third-party providers regularly conduct audits to assess the effectiveness of cybersecurity practices and ensure compliance with data protection standards.
- **Data Backup and Disaster Recovery**: The clinic ensures that regular backups are performed on patient data to protect against potential data loss or system failures. In case of a cybersecurity breach, the clinic has a comprehensive disaster recovery plan in place to ensure rapid response and data restoration.

4. Third-Party Agreements

The clinic enters into formal agreements with third-party software providers to ensure that all parties involved adhere to the same high standards of confidentiality and data protection. These agreements include provisions that:

- Limit the use of patient data to the specific purposes for which it is provided
- Require third-party providers to implement appropriate cybersecurity practices to protect patient information
- Restrict access to patient data to authorized personnel only and prohibit the unauthorized sharing or disclosure of information
- Establish protocols for responding to data breaches or security incidents

5. Patient Consent

By using the clinic's services, patients consent to the sharing of their personal and health information with third-party software providers as outlined in this policy. Patients have the right to withdraw their consent at any time, subject to the limitations of applicable laws and operational requirements. If patients wish to limit or prevent the sharing of their information with third-party providers, they must notify the clinic in writing.

6. Data Retention and Disposal

The clinic retains patient data only for as long as necessary to provide medical services, fulfill legal obligations, and meet operational needs. Upon completion of services, or when requested by the patient, data is securely deleted or anonymized in accordance with the clinic's data retention and disposal policies.

7. International Data Transfer

In some cases, third-party providers may process or store patient data outside of Australia. If this occurs, the clinic ensures that appropriate safeguards are in place to protect patient information in compliance with Australian privacy laws, including the Australian Privacy Principles (APPs).

8. Breach Notification

In the event of a data breach or security incident, the clinic will notify affected patients in accordance with the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988 (Cth). The clinic will also work with third-party software providers to mitigate any potential harm and prevent future breaches.

9. Patient Rights

Patients have the right to:

- Request access to their personal health data held by the clinic
- Request corrections to any inaccuracies in their health data
- Withdraw consent for the sharing of their data with third-party providers
- Be informed about how their data is being used, stored, and protected

By accepting the clinic's services, patients acknowledge that their personal and health information may be shared with third-party providers in accordance with the terms of this policy, and that all necessary cybersecurity measures will be taken to protect their data.

For any questions or concerns regarding the clinic's data privacy and security practices, patients are encouraged to contact the clinic directly.

Administrative Team
Dr. Bawani Marsden Clinic