

Cardinal Santos Medical Center (CSMC) values your privacy and is committed to protecting your personal data in accordance with Republic Act No. 10173, otherwise known as the **Data Privacy Act of 2012**, its Implementing Rules and Regulations, and other applicable laws and regulations. This **Data Privacy Statement** describes how the **CSMC Patient App** collects, uses, stores, processes, and protects your personal information when you access or use our services.

By using the CSMC Patient App, you acknowledge that you have read, understood, and agreed to the terms of this Statement.

This Data Privacy Statement applies to all users of the CSMC Patient App and covers all personal data and sensitive personal information collected, whether manually or electronically, in connection with your use of the app and the healthcare services facilitated through it.

When We Collect Your Data. We collect your personal data at the following stages:

1. **Upon Account Registration.** When you first sign up and provide identification and contact details.
2. **When Using App Features.** Booking appointments, initiating eConsults, viewing records, or submitting forms.
3. **During Medical Interactions.** When your healthcare provider updates your medical records in hospital systems connected to the app.
4. **When Contacting Us.** Through in-app chat, calls, or emails for inquiries or support.
5. **During App Use.** Automatically collected usage analytics and technical data.

Types of Data We Collect

1. **Personal Information.** When you register your account, we collect your name, email address, phone number, date of birth, gender, and other relevant demographic information.
2. **Sensitive Personal Information.** We may collect health-related information such as medical history, clinical results, and other health records to provide personalized healthcare services.
3. **Usage and Technical Data.** We gather data about your interactions with the app, including app usage statistics, navigation patterns, and device information (e.g., device type, operating system).

How Your Personal Data is Used. Your personal and health information is processed for the following **specific purposes**:

1. **To Provide Healthcare Services**
 - a. Enable appointment scheduling, consultations (onsite and virtual), follow-ups, and procedure tracking

- b. Allow access to medical records including lab results, prescriptions, and imaging reports
 - c. Coordinate care between departments and clinicians to ensure continuity of treatment
 - d. Facilitate prescription management and health monitoring
- 2. **To Enable Effective Communication**
 - a. Send appointment reminders, lab result availability notifications, and follow-up instructions
 - b. Respond to queries, feedback, or support concerns through various communication channels
 - c. Share relevant health education, system announcements, or wellness programs
- 3. **To Maintain System Functionality and Improve Services**
 - a. Analyze usage data to improve app performance and usability
 - b. Conduct app analytics to enhance service delivery, content accuracy, and feature relevance
 - c. Address bugs, crashes, or system downtime
- 4. **To Ensure Legal and Regulatory Compliance**
 - a. Report required data to public health authorities, insurance providers, or legal institutions when mandated
 - b. Assist in medical audits or official investigations, when legally obligated
- 5. **To Protect Life and Safety**
 - a. In urgent or emergency cases, access to data may be used to prevent significant health risks, especially if the user is incapacitated or unable to consent

Legal Basis for Processing. We process your personal and health information based on the following lawful grounds:

- a. **Your Consent**
- b. **Fulfillment of a Contract** (healthcare service delivery)
- c. **Compliance with Legal Obligations**
- d. **Protection of Vital Interests**
- e. **Legitimate Interests** (e.g., service optimization, security)

Data Retention. We retain your data for fifteen (15) years or for as long as necessary to fulfill the above purposes, comply with applicable laws, or until the data is no longer relevant. After this period, personal data is securely deleted, archived, or anonymized.

Data Security and Privacy. We prioritize the security and privacy of your data through the following measures:

- a. **Encryption.** We encrypt data transmissions using industry-standard protocols (e.g., HTTPS, TLS) to protect data in transit. Data stored in our servers is encrypted at rest using strong encryption algorithms.
- b. **Access Control.** We implement strict access controls and authentication mechanisms to ensure that only authorized personnel have access to your PHI.
- c. **Data Minimization.** We collect and retain only the minimum necessary data required for app functionality and service delivery. We do not share your data with third parties without your explicit consent, except as required by law or regulatory obligations.
- d. **Security Monitoring.** Our systems are regularly audited and monitored for vulnerabilities.
- e. **Backup and Recovery.** We maintain secure backups and recovery mechanisms to protect your data from loss.

Data Sharing and Disclosure. Your data is shared only under the following conditions:

- a. **With Your Consent** – To physicians, specialists, or relatives you authorize
- b. **With Authorized CSMC Healthcare Providers** – For continuity of care
- c. **With Third-Party Vendors** – For services like cloud hosting, under strict confidentiality and data processing agreements
- d. **With Government or Regulatory Authorities** – When legally required
- e. **In Emergencies** – To protect life or prevent serious harm

CSMC does **not** sell or disclose your data to advertisers or marketers.

Your Rights as a Data Subject. You have the following rights under the Data Privacy Act:

- **Right to Be Informed**
- **Right to Access**
- **Right to Object**
- **Right to Erasure or Blocking**
- **Right to Rectification**
- **Right to Data Portability**
- **Right to Lodge a Complaint** with the **National Privacy Commission (NPC)**

To exercise your rights, please contact our Data Protection Officer (DPO).

Data Breach Notification. In the event of a personal data breach, CSMC will notify affected users and the National Privacy Commission (NPC) within seventy-two (72) hours, in accordance with applicable laws. Appropriate remedial actions will be implemented immediately to mitigate risks.

Updates to This Statement. This Statement may be updated to reflect changes in regulations, technology, or services. We will notify users of any significant revisions through the app or official channels.

Last Updated: [Insert Date of Last Revision]

For questions, feedback, or requests related to your personal data, please contact:

Data Protection Officer

Cardinal Santos Medical Center

Greenhills, San Juan City, Metro Manila, Philippines

Tel: (02) 8727 0001 loc 3070

Email: dpo@csmc.ph