

Website Privacy Policy & PDPA Compliance Statement

Effective Date: September 30, 2026 | Managed by Clinic Data Protection Officer

1. Introduction & Scope

At MyBracesClinic, patient privacy and clinical data security are fundamental tenets of our operations. This Privacy Policy outlines how we collect, utilize, disclose, and protect your Personal Data in strict compliance with the Singapore Personal Data Protection Act (PDPA) and the Ministry of Health (MOH) regulatory frameworks.

2. Mandatory Collection of Full NRIC / FIN Numbers

Unlike typical retail or commercial businesses which are prohibited from collecting national identifiers under general PDPA guidelines, **licensed healthcare providers are explicitly required and permitted by law** to collect, process, and record full NRIC, FIN, or Passport numbers. This is governed under the following critical mandates:

- **Absolute Patient Identification:** To eliminate the catastrophic risks of medical or clinical mix-ups (such as wrong-patient surgical procedures, misallocated diagnostic X-rays, or life-threatening medication/allergy mismatches).
- **National Electronic Health Record (NEHR) Synchronization:** To securely report, index, and query your electronic health files within the central healthcare ecosystem managed by Synapse.
- **Subsidy and Financial Verification:** To process your medical claims, insurance validations, and government subsidies under schemes such as CHAS, MediSave, and Pioneer/Merdeka Generation benefits.

3. Specific Purposes of Data Use

Your personal and clinical data will strictly be utilized to provide direct patient care, coordinate clinical referrals with external specialists, process administrative payments, and fulfill statutory medical reporting duties. We maintain a zero-tolerance policy against commercial data exploitation; your data will never be sold, leased, or extracted for unrelated third-party marketing campaigns.

4. Data Protection & Encryption Safeguards

All physical records are logged immediately and returned without delay. Electronic data records—including full national identifiers and dental treatment profiles—are securely housed in an encrypted, password-protected Clinic Management System (CMS) featuring real-time electronic access tracking and strict credential controls.

1. Introduction & Scope

At My Dental Team, patient privacy and clinical data security are fundamental tenets of our operations. This Privacy Policy outlines how we collect, utilize, disclose, and protect your Personal Data in strict compliance with the Singapore Personal Data Protection Act (PDPA) and the Ministry of Health (MOH) regulatory frameworks.

2. Mandatory Collection of Full NRIC / FIN Numbers

Unlike typical retail or commercial businesses which are prohibited from collecting national identifiers under general PDPA guidelines, **licensed healthcare providers are explicitly required and permitted by law** to collect, process, and record full NRIC, FIN, or Passport numbers. This is governed under the following critical mandates:

- **Absolute Patient Identification:** To eliminate the catastrophic risks of medical or clinical mix-ups (such as wrong-patient surgical procedures, misallocated diagnostic X-rays, or life-threatening medication/allergy mismatches).
- **National Electronic Health Record (NEHR) Synchronization:** To securely report, index, and query your electronic health files within the central healthcare ecosystem managed by Synapse.
- **Subsidy and Financial Verification:** To process your medical claims, insurance validations, and government subsidies under schemes such as CHAS, MediSave, and Pioneer/Merdeka Generation benefits.

3. Specific Purposes of Data Use

Your personal and clinical data will strictly be utilized to provide direct patient care, coordinate clinical referrals with external specialists, process administrative payments, and fulfill statutory medical reporting duties. We maintain a zero-tolerance policy against commercial data exploitation; your data will never be sold, leased, or extracted for unrelated third-party marketing campaigns.

4. Data Protection & Encryption Safeguards

All physical records are logged immediately and returned without delay. Electronic data records—including full national identifiers and dental treatment profiles—are securely housed in an encrypted, password-protected Clinic Management System (CMS) featuring real-time electronic access tracking and strict credential controls.