

PATIENT & PUBLIC PRIVACY NOTICE

Transparency Declaration Pursuant to Republic Act No. 10173 (Data Privacy Act of 2012)

Effective Date: August 26, 2026

This Privacy Notice explains how our clinic platform collects, uses, protects, and discloses your personal data and sensitive health records when you receive medical services or access our system.

1. WHAT DATA WE COLLECT

- **Personal Identification:** Full name, contact numbers, home address, birthdate, gender.
- **Sensitive Health Information:** Medical histories, clinical notes, diagnosis, prescriptions, laboratory results, treatment plans, odontogram/dental charting, and any documents you or your clinic upload to your record (e.g. referrals, prior records, images).
- **Technical Data:** System access logs, audit trails, and authentication timestamps, kept to detect and investigate unauthorized access to your record.

2. PURPOSE OF DATA COLLECTION

Your data is processed strictly for legitimate healthcare purposes, including providing medical consultations, maintaining clinical records, facilitating clinic operations, managing medical billing, and fulfilling statutory health reporting obligations.

3. HOW WE PROTECT YOUR DATA

We implement strict physical, organizational, and technical security controls, including:

- Encryption of patient records at rest and encryption of all data in transit (HTTPS/TLS) between your browser and our servers.
- Optional multi-factor authentication (MFA) for every staff and administrator account, as an additional sign-in step beyond a password.
- Per-clinic data isolation: every account is scoped to its own clinic, so staff at one clinic cannot access another clinic's patient records, regardless of physical location.
- Role-based access control, so each staff account can only reach the parts of the system its role actually needs.
- Rate limiting and automatic account lockout on repeated failed sign-in attempts, to resist unauthorized access attempts.
- Regular automated backups with point-in-time recovery, plus an independent backup copy kept separately from the primary system, so records can be restored in the event of accidental loss or a system failure.
- A recorded audit trail of access to patient records, reviewed to detect and investigate unauthorized activity.

4. SHARING & DISCLOSURE

We do not sell or market your personal health data. Data is only shared with authorized clinic personnel treating you, third-party service providers (such as cloud hosting and infrastructure providers) operating

under strict confidentiality and data processing agreements, or government authorities when explicitly mandated by Philippine law.

5. YOUR PRIVACY RIGHTS

As a Data Subject under RA 10173, you hold statutory rights to be informed, access your records, request correction of inaccurate data, request data erasure where legally permissible, and lodge complaints with the National Privacy Commission (NPC).

CONTACT OUR PRIVACY OFFICE

**Data Protection Officer
(DPO) Email** dataprivacy@dmdent.com

Contact Number 09052314996

Physical Address 207 La Frontera Bldg, San Jose Residencias Balibago Santa Rosa
City Laguna