CALL DOC — Health Data Hosting Policy

POLICY ON THE HOSTING HEALTH DATA

CALL DOC Telemedicine Platform — MOROCCO

Document Reference: CLDOC-HDS-MA | Version 1.0 | April 2026

Health data constitutes sensitive personal data that is subject to enhanced protection under Moroccan law. This policy describes the technical, organizational, and legal safeguards implemented by CALL DOC to ensure the security, confidentiality, and integrity of your health data.

This Policy is governed by ***Framework Law No. 06-22 on the National Health System (Dahir No. 1-22-77 of December 9, 2022), Law No. 131-13 (Practice of Medicine), Law No. 09-08 (protection of personal data), Law No. 53-05 (electronic data exchange), the Code of Ethics of the Medical Profession (Decree No. 2-21-225 of June 17, 2021), Decree No. 2-18-378 of July 25, 2018 (practice of telemedicine), Decree No. 2-20-675 of January 22, 2021, and all applicable Moroccan laws and regulations.***

1. IDENTITY AND RESPONSIBILITIES

Data Controller	CALL DOC — Limited Liability Company with capital of 100,000.00 MAD
ICE Number	003900577000037
RC Number	177405 — Marrakech Commercial Court
Headquarters	Located at: Apartment 15, Building 12, Sine Housing Development, Allal El Fassi Avenue, Marrakech, Morocco
Co-managers	Milouda Kheira Miloudi, née Muths, and Antoine Jean François Muths
Data Protection Officer	privacy@calldoc.ma
Phone	+212 6 95 18 80 33
CNDP Declaration	Made in accordance with Law No. 09-08

2. NATURE OF THE HEALTH DATA HOSTED

As part of the provision of its telemedicine services, CALL DOC hosts the following categories of health data:

Patient Clinical Data

- Reasons for consultation and symptoms reported by the patient
- Medical history, allergies, and current treatments
- Teleconsultation reports written by the physician
- Electronic prescriptions issued via the Platform
- Test results and attachments shared during the consultation
- Biometric data transmitted via connected devices (if applicable, subject to the patient's explicit consent)

Administrative and Traceability Data

- Identifiers of doctors and patients associated with each consultation
- Consultation timestamps (date, time, duration)
- Medical record access logs (access tracking)

- Billing data related to medical procedures

No health data is used for commercial, advertising, or profiling purposes. Access to clinical data is strictly limited to the treating physician and the patient concerned.

3. DATA LOCATION AND SOVEREIGNTY

CALL DOC is committed to ensuring that its patients' health data is primarily hosted on infrastructure located within the territory of the Kingdom of Morocco, in accordance with the requirements of Law No. 09-08 and the recommendations of the CNDP.

Primary Location	Kingdom of Morocco
Host	Oracle Cloud Infrastructure (OCI) — data and application located in Morocco
Backup location	Kingdom of Morocco (disaster recovery site)
Transfers outside Morocco	Only with CNDP guarantees and explicit consent
Monitoring	24/7

In the event that data transfer to a third country is necessary due to technical constraints, CALL DOC ensures that the destination country offers an adequate level of protection recognized by the CNDP, or that appropriate contractual safeguards (standard contractual clauses) are in place. You will be notified of any transfer.

Legal basis: Law No. 09-08 (Art. 43 et seq.).

4. TECHNICAL SECURITY MEASURES

Data Encryption

- End-to-end encryption of data in transit: TLS 1.2 protocol minimum (TLS 1.3 recommended)
- Encryption of data at rest: AES-256 algorithm
- Encryption of backups with keys managed separately from the data
- Secure communication channels for telemedicine consultations (encrypted video/audio)

Access Control

- Multi-factor authentication (MFA) required for all access to health data
- Role-Based Access Control (RBAC): each user accesses only the data necessary for their role
- Strict patient data segregation: a doctor can only access the records of their own patients
- Quarterly review of access rights and immediate removal of obsolete access
- Logging of all access to health data (who, what, when)

Monitoring and Detection

- Real-time monitoring of hosting infrastructure (24/7)
- Active intrusion detection system (IDS/IPS) on all servers
- Regular security audits and penetration tests (at least once a year)
- Automatic alerts in the event of abnormal access or intrusion attempts
- Documented and regularly tested incident response plan

💾 Continuity and Backup

- Daily automatic backups of health data
- Backups retained for a minimum of 30 days
- Disaster recovery plan (DRP) with a recovery time objective of less than 4 hours
- Geographically separate backup site to ensure service continuity
- Backup restoration tests performed quarterly

5. ORGANIZATIONAL SECURITY MEASURES

5.1 Personnel and Training

- Only strictly authorized personnel have access to health data (principle of least privilege)
- Every staff member with access to health data is subject to a contractual confidentiality obligation
- Mandatory training on personal data protection and cybersecurity for all staff
- Departure management procedure: immediate revocation of access upon contract termination

5.2 Subcontractors and Service Providers

- Any technical service provider accessing health data is bound by a data processing agreement in accordance with Law No. 09-08
- Service providers undergo a preliminary security assessment and periodic audits
- The list of authorized subcontractors is kept up to date and is available upon written request to privacy@calldoc.ma

5.3 Incident Management

In the event of a health data breach, CALL DOC follows this procedure:

Within 24 hours	Identification and containment of the incident — activation of the crisis response team
Within 48 hours	Assessment of the impact and the data involved
Within 72 hours	Notification to the CNDP in accordance with Law No. 09-08
Without undue delay	Notification to affected patients if the incident poses a high risk to their rights

6. RETENTION PERIODS FOR HEALTH DATA

CALL DOC applies the following retention periods, in accordance with Moroccan legal obligations:

Medical records and consultation reports	10 years from the last consultation (Law No. 131-13)
Electronic medical prescriptions	10 years
Access and audit logs	3 years
Billing data related to medical services	10 years (CGI — Art. 211)
Data deleted at the patient's request	30 days after the request is approved, subject to legal retention obligations

Upon expiration of the retention periods, health data is securely and irreversibly destroyed (multiple overwriting of storage media, physical destruction if necessary) or permanently anonymized for statistical purposes.

Legal basis: Law No. 09-08 (Art. 5); Law No. 131-13; General Tax Code (Art. 211).

7. PATIENTS' RIGHTS REGARDING THEIR HEALTH DATA

As a patient, you have the following rights regarding your health data hosted by CALL DOC:

Right of access	Obtain a copy of your hosted health data — response time: 30 days
Right to rectification	Correct any inaccurate data in your medical record
Right to erasure	Request the deletion of your data, subject to legal retention requirements (10 years)
Right to object	Object to certain non-medical processing of your data
Right to data portability	Receive your data in a structured, machine-readable format

To exercise your rights, submit the rights exercise form available in the "Exercise My Rights" section on the Site, or contact us at privacy@calldoc.ma. Response time: 30 calendar days.

8. AUDIT AND COMPLIANCE

- CALL DOC has filed the required declarations with the CNDP in accordance with Law No. 09-08
- An internal compliance audit is conducted annually
- External security audits are conducted by independent specialized service providers
- The results of the audits are communicated to management and result in a corrective action plan
- CALL DOC cooperates fully with the CNDP in the context of its oversight activities

A copy of the CNDP declaration receipt is available upon written request to privacy@calldoc.ma.

9. CONTACT — DATA PROTECTION OFFICER

For any questions regarding the hosting and security of your health data:

Email	privacy@calldoc.ma
Phone	+212 6 95 18 80 33
Mailing Address	CALL DOC — Apartment 15, Building 12, Sine Housing Development, Allal El Fassi Avenue, Marrakech, Morocco
CNDP (complaint)	www.cndp.ma | contact@cndp.ma | Avenue AL ARZ, Sector 4, M1, HAY RIAD, Rabat

10. POLICY UPDATES

This Health Data Hosting Policy is reviewed at least once a year or whenever there is a significant change in applicable regulations or hosting infrastructure. Substantial changes are communicated to users via email and through a notification on the Platform at least thirty (30) days before they take effect.

CALL DOC COMMITMENT

CALL DOC is committed to maintaining the highest level of security for the hosting of your health data, to strictly complying with applicable Moroccan regulations, and to promptly informing you of any incident that may affect your data. The trust you place in us by sharing your health data is our top priority.

CALL DOC – Morocco / Law No. 06-22 / Law No. 131-13 / Law No. 09-08 / Law No. 53-05 / Code of Medical Ethics / Decree No. 2-18-378 / Decree No. 2-20-675 / CGI / DOC / Penal Code

CLDOC-HDS-MA v1.0 | Confidential | April 2026