DoctorsHub24 HealthTech Limited

Reg: C-194820/2026 (RJSC, Dhaka, Bangladesh) | e-TIN: 482910482911 | VAT BIN: 00519
HQ: House 24, Road 11, Banani, Dhaka-1213, Bangladesh
Hubs: Dhaka (BD) | Riyadh (SA) | Kuala Lumpur (MY) | Dubai (AE) | Tel: +8801896042360

DOC: DH24-LEG-06 (v2.4-BD)
REF: DH24-LEG-06-MASTER-2026
Effective: 2026-11-11
doctorshub24.com

Medical Data Security & Breach Response Policy

Technical Safeguards, RBAC Access Control, Audit Logging & 72-Hour Cyber Incident SOP (Bangladesh)

Governing Law: Cyber Security Act 2023 (Bangladesh); BGD e-GOV CIRT Incident Reporting Protocols; ICT Act 2006 (Sec. 54-67); ISO/IEC 27001 & HIPAA-Inspired Health Safeguards.

Jurisdiction & Seat:	Dhaka, People's Republic of Bangladesh
Operating Markets:	Bangladesh (BD) | Saudi Arabia (SA) | Malaysia (MY) | UAE (AE)
Live Commission Rules:	Consult: Doctor 35% / Hosp 40% / Platform 10% | Labs: Hosp 55...
System Compliance Posture:	Hold: 30m | Retention: 1825 days | Currencies: BDT, USD, SAR,...

EXECUTIVE OVERVIEW

Documents DoctorsHub24 cryptographic & RBAC architecture (BCrypt/Argon2, TOTP 2FA, login throttling, CSRF tokens, audit trails) plus mandatory containment and 72-hour breach disclosure SOP.

1. Architectural Access Control & Role Isolation (RBAC)

DoctorsHub24 HealthTech Limited enforces strict role-segregated authentication sessions across Superadmin (admin/), Hospital (hospitals/), Doctor (doctors/), Pharmacy (pharmacy/), Agent (agents/), and Patient (user/) portals via auth_guard policies. Cross-tenant queries require explicit ownership or verified care relationship.

2. Authentication Hardening, CSRF, Brute-Force & Document Isolation

Technical controls deployed in production include: (i) strong adaptive password hashing; (ii) mandatory/supported Time-Based One-Time Password 2FA (‘user_totp‘); (iii) automated IP & account login throttling (‘login_throttle‘); (iv) full login activity forensics (‘user_login_activity‘); (v) cryptographic CSRF protection on state-changing POST forms; and (vi) prepared PDO SQL statements preventing injection.

3. Transport Encryption, Medical Upload Sanitation & Backup Governance

All portal traffic mandates TLS/HTTPS encryption. Uploaded prescriptions, diagnostic PDFs, KYC licenses, and medical tourism passports undergo MIME/size validation, non-executable storage isolation, and scheduled database/upload backups via Admin Backups (admin/backup.php).

4. Security Incident Classification & Containment (0-24 Hours)

Upon detection of suspected unauthorized PHI access, credential compromise, ransomware, or anomalous API scraping, the Incident Response Lead immediately revokes affected tokens/sessions, isolates impacted nodes, preserves immutable forensic logs, and initiates root-cause containment within 4 hours.

5. Regulatory & User Breach Notification Protocol (Within 72 Hours)

In alignment with Bangladesh Cyber Security Act 2023 and BGD e-GOV CIRT coordination best practices, confirmed personal/medical data breaches posing risk to individuals must be reported to affected users, Partner Hospitals, and competent authorities within 72 hours detailing impact scope, compromised categories, and remediation steps via DPO (support@doctorshub24.com).

6. Annual Security Audits, Vulnerability Testing & Retention

System health, API rate limits, and staff privilege reviews are audited quarterly via admin/system_health.php & admin/api_security.php. Clinical logs adhere to 1825-day retention and secure cryptographic erasure upon verified deletion requests.

IN WITNESS WHEREOF, the Parties execute this Agreement in duplicate:

For: DoctorsHub24 HealthTech Limited

_____

Authorized Managing Director
Authorized Signatory & Compliance Officer
Date: _____ Place: Dhaka

For: Platform Engineering, DPO & Clini...

_____

Authorized Signature & Seal
NID / BMDC / Passport / TIN: _____
Date: _____