ITSEC

♡ Dubai Health Authority - Healthcare Cybersecurity Compliance

DHA Health Data Compliance Map

Complete Guide to Healthcare Cybersecurity Requirements for Hospitals, Clinics, Telehealth, and Health AI Systems

Edition: 2026

itsecnow.com | hello@itsecnow.com | +971.4.257.2406

Executive Summary

Understanding DHA Healthcare Cybersecurity Requirements in Dubai

What is DHA Compliance?

The Dubai Health Authority (DHA) regulates all healthcare services in Dubai under Federal Law No. (2) of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields. This law mandates comprehensive cybersecurity controls for protecting Patient Health Information (PHI), requires 25-year data retention with strict confidentiality, and governs AI applications in healthcare. All healthcare facilities must integrate with NABIDH (National Backbone for Integrated Dubai Health) for Health Information Exchange.

> **Key Insight:** DHA compliance extends beyond traditional IT security. Healthcare organizations must protect sensitive patient data for 25 years, implement consent-based access controls, and obtain pre-deployment approval for any AI-powered diagnostic or treatment systems.

Who Needs DHA Compliance?

The following entities operating in Dubai's healthcare sector must comply with DHA cybersecurity requirements:

- Hospitals & Medical Centers
- Clinics & Outpatient Facilities
- Telehealth Platforms
- Health AI/ML Systems
- Pharmacies & Labs
- Medical Device Software (SaMD)
- Health Insurance Providers
- Medical Imaging (PACS/DICOM)

> ⚠ **Regulatory Mandate:** Non-compliance with DHA health data requirements can result in license suspension, significant fines up to AED 1,000,000, and criminal penalties for serious breaches affecting patient safety.

Core Requirements Matrix

DHA cybersecurity requirements mapped to ITSEC solutions

DHA Requirement	Description	ITSEC Solution
PHI Protection	Encryption of patient health information at rest and in transit	End-to-End Encryption Audit Cryptographic controls assessment, key management review
25-Year Retention	Long-term secure storage of medical records with integrity verification	Archive Security Assessment Data lifecycle security, backup validation, integrity checks
NABIDH Integration	Secure connectivity to Dubai Health Information Exchange	API Security Testing HIE integration security, HL7/FHIR protocol testing
Consent Management	Patient consent tracking and role-based access controls	IAM Assessment Access control audit, consent workflow validation
AI Governance	Pre-deployment security for AI diagnostic/treatment systems	AI Security Audit Model security, adversarial testing, bias detection
Incident Response	Breach notification to DHA and affected patients	IR Plan Development Healthcare-specific IR procedures, tabletop exercises
Medical Imaging	PACS/DICOM security for MRI, CT, X-ray systems	Medical Device Security PACS penetration testing, DICOM protocol security

Compliance Note: All healthcare organizations must undergo annual security assessments. High-risk facilities (hospitals, telehealth platforms) should conduct semi-annual penetration testing of patient-facing systems.

Entity-Specific Requirements

Tailored compliance requirements by healthcare entity type

Hospitals & Medical Centers

- ✓ EMR/EHR system security assessment
- ✓ Medical device network segmentation
- ✓ PACS/DICOM imaging security
- ✓ Pharmacy system integration security
- ✓ Patient portal penetration testing

Telehealth Platforms

- ✓ Video consultation encryption
- ✓ Mobile app security testing
- ✓ Remote monitoring device security
- ✓ E-prescription system validation
- ✓ Patient authentication controls

Health AI/ML Systems

- ✓ AI model security assessment
- ✓ Training data protection audit
- ✓ Adversarial attack testing
- ✓ Algorithm bias detection
- ✓ Clinical decision support validation

Medical Imaging (PACS)

- ✓ DICOM protocol security testing
- ✓ Imaging archive protection
- ✓ Radiology workstation hardening
- ✓ Image transmission encryption
- ✓ MRI/CT/X-ray system security

⚠ **Medical Device Alert:** Connected medical devices (IoMT) present unique security challenges. DHA requires all networked medical devices to be assessed for vulnerabilities and isolated from general IT networks.

Compliance Implementation Timeline

Typical 12-week roadmap to DHA healthcare security compliance

● Weeks 1-2

Discovery & Gap Analysis

Comprehensive assessment of current security posture against DHA requirements. Identify PHI data flows, NABIDH integration points, and medical device inventory.

● Weeks 3-4

Risk Assessment & Prioritization

Healthcare-specific risk assessment focusing on patient safety, data confidentiality, and regulatory compliance. Prioritize remediation based on risk severity.

● Weeks 5-6

Penetration Testing

Comprehensive security testing of EMR systems, patient portals, telehealth platforms, medical devices, and NABIDH integration points.

○ Weeks 7-9

Remediation & Implementation

Address identified vulnerabilities, implement encryption controls, configure access management, and establish consent tracking mechanisms.

○ Weeks 10-11

Policy & Procedure Development

Create DHA-compliant security policies, incident response procedures, data retention policies, and patient consent management workflows.

○ Week 12

Validation & Certification

Final compliance validation, documentation package preparation, and submission to DHA for approval. Staff training on new procedures.

NABIDH Integration Security

Securing Dubai's Health Information Exchange connectivity

What is NABIDH?

The National Backbone for Integrated Dubai Health (NABIDH) is Dubai's unified Health Information Exchange platform. All DHA-licensed healthcare facilities must integrate with NABIDH to share patient health records securely. ITSEC provides specialized security testing for NABIDH integration points.

NABIDH Security Domain	ITSEC Testing Approach
API Security	HL7 FHIR API penetration testing, authentication validation, rate limiting assessment, input validation testing
Data Encryption	TLS configuration audit, certificate management review, encryption key handling assessment
Access Control	Role-based access validation, consent enforcement testing, audit trail verification
Data Integrity	Message integrity verification, tamper detection, non-repudiation controls
Availability	Failover testing, redundancy validation, disaster recovery verification

Integration Requirement: All healthcare facilities must complete NABIDH security certification before going live with the Health Information Exchange. ITSEC provides end-to-end security assessment and certification support.

Need NABIDH Security Certification?

Our healthcare security experts can guide you through the entire certification process

Schedule Assessment

Healthcare Security Self-Assessment

Evaluate your organization's DHA compliance readiness

- □ Patient health information encrypted at rest (AES-256 or equivalent)
- □ NABIDH integration security tested and certified
- □ Patient consent management system operational
- □ PACS/DICOM systems security assessed
- □ 25-year data retention policy documented
- □ AI/ML systems pre-approved by DHA
- □ Staff security awareness training conducted
- □ Telehealth platform security validated
- □ TLS 1.3 encryption for all PHI in transit
- □ Role-based access control implemented for EMR
- □ Medical devices segmented from general network
- □ Healthcare-specific incident response plan
- □ Secure backup and disaster recovery tested
- □ Annual penetration testing completed
- □ Third-party vendor security assessed
- □ Audit logging enabled for all PHI access

Scoring Guide: 14-16 checks = Strong compliance posture. 10-13 checks = Moderate gaps requiring attention. Below 10 = Significant compliance risk requiring immediate remediation.

Why ITSEC for Healthcare Security?

The trusted partner for healthcare cybersecurity in the UAE

200+ Healthcare Assessments

ISO 27001 & 27799 Certified

100% DHA Compliance Rate

0 Post-Assessment Breaches

Our Healthcare Security Services

ITSEC provides comprehensive cybersecurity services tailored for the healthcare sector:

✓ EMR/EHR Security Assessment

✓ NABIDH Integration Testing

✓ Medical Device Security

✓ PACS/DICOM Security Testing

✓ Telehealth Platform Security

✓ Health AI Security Audit

✓ PHI Encryption Assessment

✓ Healthcare VCISO Services

✓ Incident Response Planning

✓ Security Awareness Training

Start Your DHA Compliance Journey

Schedule a free consultation with our healthcare security experts

Book Assessment

Website	Email	Phone
itsecnow.com	**hello@itsecnow.com**	**+971.4.257.2406**