Sri Lanka Institute of Information Technology

Enterprise Standards for Information Security - IE3102

HHM Health Systems

ISMS Core Documentation Pack

IT Number	Student Name
IT23440418	DOJ Silva
IT23149144	G D P Nirshan
IT23238312	M A D D Sankalpana
IT23159044	S N Wickramathilaka

Table of Content

1. Scope Statement 3

2. Information Security Policy 4

3. Statement of Applicability (SoA) – HHM Health Systems 5

Excluded Controls (Examples) 6

4. Risk Treatment Plan 6

1. Scope Statement

Organization Name: HHM Health Systems

ISMS Scope:

The scope of the ISMS at HHM includes:

- All 4 hospitals, 12 clinics, and the centralized digital health hub.
- Information systems, applications, and databases storing, processing, or transmitting patient health information (PHI) and personal identifiable information (PII).
- Internet of Medical Things (IoMT) devices on hospital networks (e.g., MRI, infusion pumps, heart monitors).
- Cloud-based data centers and cloud infrastructure (used for Electronic Health Records and Telemedicine services).
- All staff, contractors, and third-party service providers processing sensitive healthcare information.

Exclusions (if any):

- Public website used for marketing (no PHI processing).
- Cafeteria management.

Scope Justification:

The scope of ISMS was defined to protect sensitive healthcare information, address regulations (HIPAA, GDPR, PDPA), and prevent cyberattacks' threats to healthcare infrastructure.

2. Information Security Policy

Policy Objective:
The policy aims at safeguarding patient health information, business information, and healthcare systems from unauthorized use, exploitation, or exposure. The policy also helps the organization to stay within compliance with the law and industry regulation.

Policy Principles:

1. Confidentiality – Patient and business data must be seen only by properly authorized individuals.
2. Integrity – Information must not be tampered with without authorization and must remain accurate.
3. Availability – Systems and services must be accessible and functional whenever the accredited users need them.
4. Compliance – The company must comply with law and standards like ISO 27001, HIPAA, GDPR, and PDPA.
5. Continuous Improvement – Security habits will be tried and improved from time to time.

Key Policy Directives:

- Employees must practice access policies (use only what you require, use secure logins).
- Patient information must be encrypted (secured) when it is stored or sent.
- Any security problems must be reported at once to the security staff.
- The third-party vendors must be screened for safety before they are employed.
- There must be yearly security training by all employees.

3. Statement of Applicability (SoA) – HHM Health Systems

Introduction

This Statement of Applicability identifies applicable Annex A controls from **ISO/IEC 27001:2022**, their implementation status, and justification for inclusion or exclusion. Controls are selected based on MSHS's healthcare environment, risk assessment, and regulatory obligations (HIPAA, GDPR, PDPA).

Control ID	Control Name	Applicability to MSHS	Implementation Justification
A.5.1	Policies for Information Security	✓ Applicable	Establishes governance across hospitals, clinics, and digital health hub.
A.5.7	Threat Intelligence	✓ Applicable	Healthcare sector is a prime target for ransomware and nation-state attacks.
A.5.23	Information Security in Supplier Relationships	✓ Applicable	Vendors handle lab systems, IoMT device servicing, and cloud hosting.
A.5.30	ICT Readiness for Business Continuity	✓ Applicable	Ensures continuity of healthcare services (24/7 availability).
A.5.36	Encryption of Information	✓ Applicable	PHI/PII must be encrypted to meet HIPAA and GDPR requirements.
A.5.37	Logging and Monitoring	✓ Applicable	Centralized SIEM deployed to monitor EHR and IoMT activity.
A.7.2	Physical Security Perimeter	✓ Applicable	Data centers, pharmacies, and critical hospital areas require restricted access.
A.7.4	Secure Disposal	✓ Applicable	Secure destruction of medical records (paper/electronic).
A.8.9	Configuration Management	✓ Applicable	IoMT devices and EHR servers require baseline secure configurations.
A.8.11	Technical Vulnerability Management	✓ Applicable	Regular patching of IoMT devices and operating systems.
A.8.12	Data Leakage Prevention (DLP)	✓ Applicable	Protects against PHI exfiltration through email or removable media.
A.8.24	Cryptographic Controls	✓ Applicable	Ensures secure encryption practices for stored and transmitted data.
A.8.28	Secure Development Life Cycle	✓ Applicable	In-house healthcare apps (EHR portal, telemedicine) require secure coding.

A.8.32	Change Management	✓ Applicable	Updates to EHR, IoMT, and clinical applications must follow structured approval.
A.8.36	Capacity Management	✓ Applicable	Healthcare systems must scale to support peak patient load.
A.8.39	Backup	✓ Applicable	Daily encrypted backups of EHR and critical systems.
A.8.40	Disaster Recovery	✓ Applicable	Hospitals need tested DR plans to ensure patient care continuity.
A.8.41	Business Continuity Readiness	✓ Applicable	Critical for uninterrupted emergency services.
A.16.1	Incident Management	✓ Applicable	Required to handle breaches, ransomware, and insider threats.
A.18.1	Compliance with Legal Requirements	✓ Applicable	Ensures HIPAA, GDPR, and local healthcare regulations are met.

Excluded Controls (Examples)

Control ID	Control Name	Exclusion Justification
A.7.9	Remote Working Security	Remote working is currently restricted for clinical staff handling PHI.
A.11.2	Off-Premises Equipment Security	No offsite equipment used for PHI processing.

4. Risk Treatment Plan

Risk Register Reference: Based on earlier gap analysis.

4.1 Risk Treatment Objectives

- ✓ Lessen the possibility and consequences of data breaches.
- ✓ Assure high system availability (hospital operations are available around-the-clock).
- ✓ Continue to abide by all applicable laws and regulations.

4.2 Risk Treatment Actions

1. **Implement ISMS Framework**
   - ✓ Create a governance framework that complies with ISO/IEC 27001:2022.
   - ✓ Establish roles and duties for information security at the clinic and hospital levels.
2. **Adopt SIEM & SOC Monitoring**
   - ✓ Install real-time server and IoMT device monitoring and centralized logging.
   - ✓ SOC will offer incident detection and reaction around-the-clock.
3. **Vendor Security Governance**
   - ✓ Assess supplier risk once a year.
   - ✓ Include security controls (incident notification, data protection) in contracts.
4. **IoMT Security Upgrades**
   - ✓ Apply medical device network segmentation.
   - ✓ Establish patching and upgrading device firmware on a regular basis.
5. **Data Encryption**
   - ✓ All hospital servers and endpoint devices are fully encrypted.
   - ✓ strong encryption standards (TLS 1.3, AES-256).
6. **Formalize Incident Response**
   - ✓ Create an incident response playbook.
   - ✓ Regular tabletop and red team exercise every year.
7. **Employee Training**
   - ✓ role-specific training annually for administrators, nurses, physicians, and IT personnel.
   - ✓ phishing campaigns to mimic phishing attacks.
8. **Continuous Improvement**
   - ✓ Every three months, ISMS is reviewed.
   - ✓ Management and internal audit reviews are done every year.