Sri Lanka Institute of Information Technology

Enterprise Standards for Information Security - IE3102

HHM Health Systems

Gap Analysis Report

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

Table of Contents

1. Organization Overview

For the purposes of this ISO/IEC 27001:2022 gap analysis project and ISMS documentation project, our team chose a fictitious healthcare organization named HHM Health Systems.

Organization Overview:

Industry: Healthcare, offered through hospitals, clinics and web health platforms.

Size: Approximately 200 employees (70 doctor, 100 nurses, 20 administrative staff, 10 IT/support staff).

Branches: Operates 2 hospitals and 5 clinics, and a central digital health hub where telemedicine and patient data are stored.

Scope: HHM handles sensitive patient data (PHI/PII), manages IoT devices and uses on-premise and cloud deployed systems to deliver health care.

This imaginary environment has been designed for our professionals to simulate and ISMS implementation following ISO/IEC 27001:2022 in a realistic approach, allowing us to do a real gap analysis, risk assessment and documentation that complies with standard.

Core Services:

- ✓ Patient care & treatment (inpatient and outpatient)
- ✓ Electronic Health Records (EHR) system
- ✓ Telemedicine & mobile health applications
- ✓ Integration with Internet of Medical Things (IoMT) devices (pacemakers, infusion pumps and patient monitoring systems)
- ✓ Cloud-based storage for health analytics

Information Security Context:

Healthcare organizations are at a great risk for:

- ✓ Sensitive information (PHI – Protected Health Information, PII – Personally Identifiable Information).
- ✓ Increase in cyberattacks (ransomware, phishing targeting hospitals).

- ✓ Compliance with HIPAA, GDPR, ISO 27001.
- ✓ Critical reliance on uptime (disruptions impact patient lives).

2. Current InfoSec Posture (Baseline Assessment)

Strengths (Current Practices):

- ✓ Centralized Electronic Health Records (EHR) with access controls.
- ✓ Firewalls, IDS/IPS, and network segmentation between the hospital, clinic, and IoT networks.
- ✓ Role-based access for doctors, nurses, and staff.
- ✓ Annual cybersecurity awareness training.
- ✓ Cloud backup of patient records.
- ✓ Simple Disaster Recovery (DR) plan.

Weaknesses (Gaps):

- ✓ No ISMS framework aligned with ISO/IEC 27001 yet.
- ✓ Patch management inconsistent → IoMT and legacy devices not always updated.
- ✓ Poor third-party/vendor risk management (outsourced lab services & cloud hosting).
- ✓ Limited incident response playbooks → not exercised ransomware recovery.
- ✓ No central logging/monitoring; no SIEM.
- ✓ No formal risk register maintained.
- ✓ Weak encryption state of IoMT devices at rest.
- ✓ Gaps in physical access controls with smaller clinics.

3. Mapping Against ISO/IEC 27001:2022

ISO/IEC 27001:2022 Clause/Control	**Requirement**	**Current Status at MSHS**	**Gap Identified**	**Recommendation**
Clause 4 – Context of the Organization	Context of the Organization Define ISMS scope, stakeholders, internal/external issues	Informally understood but undocumented	No documented ISMS scope or stakeholder analysis	Conduct stakeholder workshops & document ISMS scope
Clause 5 – Leadership	Leadership commitment, InfoSec policy	InfoSec policy exists but limited to IT staff	Lack of organization-wide InfoSec leadership & awareness	Establish CISO-led ISMS steering committee
Clause 6 – Planning	Risk assessment & treatment plan	Ad-hoc risk handling	No defined risk methodology	Adopt ISO 27005-based risk assessment process
Clause 7 – Support	Resources, awareness, communication	Training held yearly	Not role-specific, low awareness in clinics	Create tailored training programs
Clause 8 – Operation	ISMS implementation & monitoring	IT security controls in place	No evidence of ISMS process integration	Security integrated into hospital processes
Clause 9 – Performance Evaluation	Internal audits, management review	Limited external audits for HIPAA only	No ISO 27001 internal audit process	Create internal audit program
Clause 10 – Improvement	Continual improvement	Reactive fixes after incidents	No continual improvement cycle	Establish PDCA (Plan-Do-Check-Act) cycle

Annex A – A.5.1 Information Security Policy	Maintain a formal, approved InfoSec policy	Exists, but only IT-focused	Lacks organization-wide approval	Update, approve, and communicate policy org-wide
Annex A – A.5.23 Data Leakage Prevention	Data exfiltration controls	No DLP tools implemented	No DLP for EHR, IoMT	Implement DLP & email filtering
Annex A – A.5.29 Protection of PII	Privacy regulation compliance	GDPR/HIPAA compliance in progress	Weak IoMT and mobile app privacy defenses	Privacy Impact Assessments for new systems
Annex A – A.8.16 Monitoring Activities	Continuous monitoring, logging	Logs are implemented but discrete	No centralized SIEM	Implement SIEM solution
Annex A – A.8.23 Web Filtering	Web traffic filtering	Basic firewall rules	No advanced content filtering	Introduce secure web gateway
Annex A – A.8.28 Secure Coding	Security in application development	Health app development outsourced	No secure coding policy for vendors	Enforce secure coding standards

4. Summary of Findings

Non-Conformities (Major Gaps):

- Formal ISMS not available.
- Risk register and risk treatment plan not available.
- Patching of IoMT devices not consistent.
- Centralized SIEM/logging not available.
- Third-party vendor risk management poor.

Observations (Minor Gaps):

- Security training not role-specific.
- IoMT and clinic data storage encryption low.

- Incident response not being tested.

Strengths:

- Strong EHR system with access controls.
- Backup plan (cloud + on-premises).
- Cyber awareness training culture.
- Good network segmentation for IoMT devices.

5. Initial Risk Register

Risk ID	Description	Likelihood	Impact	Risk Rating	Treatment Recommendation
R1	Ransomware attack disrupting patient care	High	Critical	Very High	Implement SIEM, run incident response drills, offline backups
R2	IoMT device exploitation (unpatched)	High	High	Very High	Create patch mgmt. policy for IoMT, segment networks
R3	Insider threat (unauthorized access to PHI)	Medium	High	High	Strengthen RBAC, implement UEBA (User Entity Behavior Analytics)
R4	Data breach via third-party lab services	Medium	High	High	Vendor risk management program, SLA with security clauses
R5	Power outage impacting hospital IT	Low	High	Medium	Strengthen BCP/DR with redundant power supply

6. Risk Treatment Recommendations

1. Implement ISMS Framework (Align with ISO/IEC 27001:2022)

- **Purpose**: Create a methodical, structured approach to regulatory compliance and patient data security management.
- **Implementation Details**:
  - ✓ Describe the scope of the ISMS (e.g., hospital IT systems, IoMT devices, and patient records).

  - ✓ Create guidelines, protocols, and standards in accordance with ISO/IEC 27001:2022 specifications.
  - ✓ Perform management reviews and internal audits.
  - ✓ Assure the commitment and governance of top management.

- **Responsible Roles**: Chief Information Security Officer (CISO), IT Security Manager, Compliance Team.
- **Expected Outcome**: An integrated governance framework for regulatory compliance and patient data protection.
- **ISO/IEC 27001 Mapping**: Clauses 4–10 (ISMS framework), Annex A.5 (Policies, Organization).

2. Adopt SIEM & SOC Monitoring (Centralized Logging, 24/7 Monitoring)

- **Purpose**: Minimize the impact on hospital operations by promptly identifying and addressing cyberthreats.
- **Implementation Details**:
  - ✓ Install a system called Security Information and Event Management (SIEM).
  - ✓ Combine the logs from servers, IoMT devices, firewalls, and EHRs.
  - ✓ Create a Security Operations Center (SOC) that is supervised around-the-clock.
  - ✓ Use cases include data exfiltration efforts, anomalous login habits, and ransomware detection.
- **Responsible Roles**: SOC Analysts, Incident Response Team, IT Infrastructure Team.
- **Expected Outcome**: Proactive defense, a shorter mean time to response (MTTR), and quicker threat detection.
- **ISO/IEC 27001 Mapping**: Annex A.8 (Monitoring, Logging), Annex A.16 (Incident Management).

3. Vendor Security Governance (Third-Party Risk Assessments)

- **Purpose**: Verify that outside vendors (cloud service providers, suppliers of medical equipment) adhere to security regulations.
- **Implementation Details**:
  - ✓ Make a framework for evaluating vendor risk.
  - ✓ Sort vendors into three risk categories: critical, medium, and low.

- ✓ Implement security clauses in contracts (e.g., SLA for breach notification, HIPAA/GDPR compliance).
- ✓ Perform routine audits and demand proof of security certifications.

- **Responsible Roles**: Procurement, Legal Department, Vendor Risk Manager, CISO.
- **Expected Outcome**: Reduced exposure to supply chain attacks, improved accountability of partners.
- **ISO/IEC 27001 Mapping**: Annex A.5.19–A.5.23 (Supplier Relationships).

4. IoMT Security Upgrades (Patching, Micro-Segmentation)

- **Purpose**: Prevent exploitation of Internet of Medical Things (IoMT) devices.
- **Implementation Details**:
  - ✓ Create a patch management policy for the devices that are linked.
  - ✓ To separate IoMT networks from vital medical infrastructure, use micro-segmentation.
  - ✓ Install intrusion detection systems (IDS) designed specifically for medical equipment.
  - ✓ Keep track of every IoMT device's assets.

- **Responsible Roles**: Biomedical Engineers, IT Security Team, Device Vendors.
- **Expected Outcome**: Increased resistance to malware that targets medical devices and a smaller attack surface.
- **ISO/IEC 27001 Mapping**: Annex A.8.9 (Configuration Management), Annex A.8.11 (Technical Vulnerability Management).

5. Data Encryption (Full Disk Encryption + Key Management)

- **Purpose**: Safeguard private patient data when it's in transit and at rest.
- **Implementation Details**:
  - ✓ Install full disk encryption using AES-256 on hospital computers, servers, and mobile devices.
  - ✓ For safe data transfer between systems, use TLS 1.3.
  - ✓ Put in place a role-based access centralized Key Management System (KMS).

  - ✓ Enforce the use of the hardware security module (HSM) and change encryption keys on a regular basis.

- **Responsible Roles**: Database Administrators, IT Infrastructure Team, Security Architects.
- **Expected Outcome**: Patient data confidentiality and adherence to GDPR and HIPAA regulations.
- **ISO/IEC 27001 Mapping**: Annex A.8.24 (Cryptography), Annex A.8.25 (Key Management).

6. Formalize Incident Response (Tabletop Exercises, Red Team Tests)

- **Purpose**: Make sure you are prepared to handle ransomware and insider threats, among other hacks.
- **Implementation Details**:
  - ✓ Create a playbook-defined Incident Response Plan (IRP).
  - ✓ Perform tabletop drills that mimic data breaches and medical catastrophes.
  - ✓ To assess detection and response skills, conduct red team vs. blue team drills.
  - ✓ Establish communication guidelines for patients, regulators, PR, and the law.

- **Responsible Roles**: Incident Response Team, SOC Analysts, Legal & Compliance Team.
- **Expected Outcome**: Quicker incident recovery and less healthcare service outage.
- **ISO/IEC 27001 Mapping**: Annex A.16.1 (Incident Management), Annex A.6.7 (Threat Intelligence).

7. Employee Training (Role-Based Security Awareness)

- **Purpose**: Reduce human mistakes that frequently result in breaches, such as phishing and configuration issues.
- **Implementation Details**:
  - ✓ Provide specialized training courses for administrators, physicians, nurses, and IT personnel.
  - ✓ Run simulated phishing attacks and give immediate feedback.

  - ✓ Learn about GDPR/HIPAA requirements and how to safely handle patient records.
  - ✓ Update training every three months to reflect emerging risks.

- **Responsible Roles**: HR, Security Awareness Team, Department Heads.
- **Expected Outcome**: Better awareness of compliance, a stronger human firewall, and a lower chance of insider threats.
- **ISO/IEC 27001 Mapping**: Annex A.6.3 (Awareness, Education, Training).

8. Continuous Improvement (Quarterly InfoSec Reviews)

- **Purpose**: Make sure ISMS adapts to new business requirements and threats.
- **Implementation Details**:
  - ✓ Review ISMS performance with senior management every three months.
  - ✓ Track KPIs such as MTTR, compliance audit scores, and the number of incidents found.
  - ✓ Incorporate input from threat intelligence reports, audits, and occurrences.
  - ✓ Use the Plan-Do-Check-Act (PDCA) cycle to make improvements over time.
- **Responsible Roles**: ISMS Steering Committee, CISO, Compliance Officers.
- **Expected Outcome**: Robust, flexible security posture in line with the changing threats facing the healthcare industry.
- **ISO/IEC 27001 Mapping**: Clause 10 (Improvement), Annex A.5.35 (Performance Evaluation).