

Week 7. Conducting Risk Assessment
Healthcare Management System (MediCare Solutions)

Janki Patel	2520611
Nirav Thummar	2537379
Sameer Sukhadiya	253660

1. System Overview

MediCare Solutions operates an integrated Electronic Health Records (EHR) system that stores and processes sensitive patient information, including medical histories, lab results, prescriptions, appointment schedules, and treatment plans. The system is accessed by clinicians, administrative staff, laboratory personnel, and external vendors.

Because the system handles regulated health data, it faces significant cybersecurity, operational, compliance, and clinical risks.

2. Purpose of the Risk Assessment

The aim of this assessment is to:

- Identify potential threats and vulnerabilities affecting the EHR system
- Evaluate the likelihood and impact of each risk
- Determine existing controls and additional mitigation measures
- Assign responsibility and timelines for remediation
- Establish residual risk levels after controls are applied

This ensures MediCare Solutions maintains confidentiality, integrity, and availability of patient data.

3. Risk Assessment Methodology

The assessment follows a standard healthcare risk management approach:

Step 1 — Identify Assets

- EHR database
- Patient records
- Medical devices connected to the network
- APIs and interfaces
- Staff accounts
- Physical devices (laptops, tablets, workstations)

Step 2 — Identify Threats

- Cyberattacks (ransomware, phishing, unauthorized access)
- Insider misuse
- System downtime
- Data inaccuracies
- Third-party vendor failures
- Physical theft
- Misconfigured medical devices or APIs

Step 3 — Identify Vulnerabilities

- Weak access controls
- Outdated software
- Insufficient monitoring
- Human error
- Misconfigured systems
- Lack of segmentation
- Inadequate vendor oversight

Step 4 — Risk Scoring

Risk Score = **Likelihood** × **Severity** Scale: 1–5 Risk Levels: **Low, Medium, High**

Step 5 — Residual Risk

Calculated after additional controls are implemented.

4. Risk Management Register — MediCare Solutions (EHR System)

Risk ID	Hazard / Risk Description	Who Is at Risk	Category	Sub-Category	Likelihood (1–5)	Severity (1–5)	Risk Score (L × S)	Risk Level	Existing Controls	Additional Controls Needed	Responsible Person	Target Date	Residual Likelihood (1–5)	Residual Severity (1–5)	Residual Risk Score	Residual Risk Level	Status
HM-S-01	Unauthorized access to patient EHR data	Patients, clinicians	Cybersecurity	Access Control	3	5	15	High	MFA, RBAC, audit logs	Biometric authentication	IT Security Manager	30/08/2026	1	4	4	Low	In progress
HM-S-02	Ransomware attack on EHR servers	Entire organisation	Cybersecurity	Malware	4	5	20	High	Endpoint protection, backups	Network segmentation, offline vault	Cybersecurity Lead	15/09/2026	2	4	8	Medium	Planned

Risk ID	Hazard / Risk Description	Who Is at Risk	Category	Sub-Category	Likelihood (1-5)	Severity (1-5)	Risk Score (L x S)	Risk Level	Existing Controls	Additional Controls Needed	Responsible Person	Target Date	Residual Likelihood (1-5)	Residual Severity (1-5)	Residual Risk Score	Residual Risk Level	Status
HS-03	System downtime affecting patient care	Patients, clinicians	Operational	System Availability	3	4	12	Medium	Redundant servers, failover	Real-time monitoring	IT Operations Lead	01/10/2026	2	3	6	Low	In progress
HS-04	Incorrect data entry leading to wrong treatment	Patients	Clinical	Data Accuracy	2	5	10	Medium	Staff training, validation checks	Clinical decision support	Clinical Governance Officer	20/08/2026	1	4	4	Low	Ongoing
HS-05	Data breach due to third-party vendor	Patients, organisation	Compliance	Third-Party Risk	3	5	15	High	Vendor contracts, assessments	Annual security audits	Compliance Manager	05/09/2026	2	4	8	Medium	Planned
HS-06	Loss of patient data due to storage failure	Patients, clinicians	Operational	Data Management	2	5	10	Medium	Daily backups, replication	Immutable storage	IT Admin	10/09/2026	1	3	3	Low	Completed

Risk ID	Hazard / Risk Description	Who Is at Risk	Category	Sub-Category	Likelihood (1-5)	Severity (1-5)	Risk Score (L x S)	Risk Level	Existing Controls	Additional Controls Needed	Responsible Person	Target Date	Residual Likelihood (1-5)	Residual Severity (1-5)	Residual Risk Score	Residual Risk Level	Status
HMS-07	Insider threat accessing sensitive records	Patients, organisation	Cybersecurity	Insider Risk	3	4	12	Medium	Access monitoring, HR checks	Behavioural analytics	Security Analyst	25/09/2026	2	3	6	Low	In progress
HMS-08	Outdated medical devices connected to network	Patients, clinicians	Technical	IoT/Medical Devices	4	4	16	High	Network isolation, patching	Zero-trust architecture	Network Engineer	30/09/2026	2	3	6	Low	Planned
HMS-09	Exposure of lab results due to misconfigured APIs	Patients	Cybersecurity	Application Security	3	5	15	High	API gateway, authentication	API penetration testing	Dev Ops Lead	18/09/2026	1	4	4	Low	In progress

5. Summary of Findings

- High-risk areas include ransomware, unauthorized access, outdated medical devices, and API misconfigurations.
- Operational risks such as downtime and data loss remain significant but manageable with improved monitoring and storage controls.
- Compliance risks from third-party vendors require stronger oversight and annual audits.
- Residual risks are mostly reduced to low or medium after additional controls.

6. Recommendations

- Strengthen identity and access management (IAM)
- Implement zero-trust security for medical devices
- Conduct regular penetration testing on APIs
- Improve vendor risk management
- Enhance monitoring and incident response capabilities
- Increase staff training on data accuracy and security awareness