SOEN6841: Software Project Management

Winter 2025

RISK ASSESSMENT AND MITIGATION

FOR

AI-DRIVEN HEALTH MONITORING APP

Date of Submission: March 23, 2025

Submitted to:

JOUMANA DARGHAM

Team Information

Student Name	Student ID
Jayanth Apagundi	40291184
Priyadarshine Kumar	40293041
Swathi Priya Pasumarthy	40322468
Jayasurya Pazhani	40289512

6. Risk Assessment and Mitigation

1. Risk Identification:

Objective:

Detecting potential risks is a crucial part for the successful development and deployment of an AI-Driven Health Monitoring App. The risks are categorized into 3 different types namely Operational, Technical and Economic risks.

Technical Risks:

- **Data Privacy and Security:** Unauthorised access to private health information may violate laws such as HIPAA and result in privacy violations.
- **System Reliability:** Patient safety may be jeopardised if technical malfunctions or errors in health monitoring result in incorrect diagnoses or missed notifications.
- **Algorithm Bias:** Certain people may suffer as a result of inequitable health advice generated by AI models trained on biassed data.

Operational Risks:

- **Integration with Healthcare Systems:** Workflows may be disrupted by difficulties integrating the app with current Electronic Health Records (EHR) systems.
- **User Adoption:** The efficacy of the app may be limited by patients' and healthcare professionals' reluctance to trust or utilise AI-driven health technologies.
- **Regulatory Compliance:** Navigating complex healthcare regulations may delay deployment or necessitate major software changes.

Economic Risks:

- **Development Costs:** Unexpected technical difficulties could cause development costs to exceed the allocated budgeted amount.
- **Return on Investment (ROI):** Financial sustainability may be impacted if user adoption rates are overestimated and the ROI is lower than anticipated.
- **Market Competition:** The profitability of the app may be impacted if new competitors with similar features take market share.

2. Risk Impact Analysis:

Prioritising mitigation activities is aided by evaluating the possible impact of risks that have been identified.

Technical Risks:

- **Data security and privacy**: Significant impact due to possible legal fines and eroded user confidence.
- **System Reliability:** High effect since patient health outcomes might be directly impacted by unreliable systems.
- **Algorithmic bias:** Moderate to high impact, since patients may suffer and reputational harm may result from biassed suggestions.

Operational Risks:

- **Integration with Healthcare Systems:** High impact since ineffective integration can disrupt clinical workflows and reduce efficiency.
- **User Adoption:** Moderate impact, The app's efficiency and reach may be limited by low adoption rates.
- **Regulatory Compliance:** High impact because of possible legal issues and delays in operations.

Economic Risks:

- **Market Competition:** Moderate impact; competition can affect revenue and market positioning.
- **Return on Investment (ROI):** High impact if the app doesn’t meet estimated financial goals.
- **Development Costs:** Moderate impact; Financial resources may be strained by budget overruns.

Risk Assessment Table:

Risk Category	Specific Risk	Impact Level	Likelihood of Occurrence
Technical	System Reliability and Performance Issues	High	Medium
Technical	Data Privacy and Security Breaches	High	Medium
Technical	Algorithmic Bias in Health Recommendations	High	Medium
Operational	Compliance with Evolving Healthcare Regulations	High	Medium
Operational	Integration Challenges with Healthcare Systems	High	Medium
Operational	Low User Adoption by Patients and Providers	Medium	High
Economic	Uncertain Return on Investment	High	Medium
Economic	Escalating Development and Maintenance Costs	High	Medium
Economic	Competitive Market Dynamics	Medium	Medium

Impact vs. Likelihood of Occurrence: Qualitative Assessment Table

Impact Level	Likelihood of Occurrence	Risk Exposure Points
High	High	9
High	Medium	6

High	Low	3
Medium	High	6
Medium	Medium	4
Medium	Low	2
Low	High	3
Low	Medium	2
Low	Low	1

Quantitative Model:

Total Risk Exposure Points = 6 (System Reliability Issues) + 6 (Data Privacy and Security Breaches) + 6 (Algorithmic Bias) + 6 (Regulatory Compliance) + 6 (Integration Challenges) + 6 (Low User Adoption) + 6 (Uncertain ROI) + 6 (Development Costs) + 4 (Market Competition) + = 52

Dollar Allocation for Each Risk Based on Contingency Fund:

Assuming a total contingency fund of $15,600, the dollar allocation for each risk is calculated as below,

Dollar Value for Risk = (Risk Exposure Points for Risk / Total Risk Exposure Points) × Total Contingency Fund

Specific Risk	**Risk Exposure Points**	**Dollar Allocation**
System Reliability and Performance Issues	6	$1,800
Data Privacy and Security Breaches	6	$1,800

Algorithmic Bias in Health Recommendations	6	$1,800
Compliance with Evolving Healthcare Regulations	6	$1,800
Integration Challenges with Healthcare Systems	6	$1,800
Low User Adoption by Patients and Providers	6	$1,800
Uncertain Return on Investment	6	$1,800
Escalating Development and Maintenance Costs	4	$1,200
Competitive Market Dynamics	6	$1,800

Note: Dollar Allocations are rounded off to the nearest hundred.

4. Risk Mitigation Strategies:

Implementing proper measures can lessen the impact and probability of identified risks.

Technical Risks:

- **System Reliability:** Establish continuous monitoring & quality assurance protocols which will help in maintaining integrity of the system.
- **Data Privacy and Security:** Implement encryption, access limitations, and frequent security audits to protect user data.
- **Algorithmic Bias:** To ensure an equitable AI performance, use a variety of training datasets and carry out bias checks.

Operational Risks:

- **Regulatory Compliance:** Keep up with changes in regulations and ensure that compliance checks are implemented at each and every stage of development.

- **Integration with Healthcare Systems:** Work together with the IT departments of healthcare facilities to ensure seamless integration & compatibility.
- **User Adoption:** Build trust and encourage adoption by educating and training stakeholders.

Economic Risks:

- **Development Costs:** Use agile project management to find problems early and fix them while keeping costs under control.
- **Return on Investment (ROI):** Conduct market research to establish realistic adoption targets and budget predictions.
- **Market Competition:** Make the software unique from other competitors by having exceptional user experience and different features.

5. Contingency Plans

Preparing for potential risk events guarantees prompt and efficient responses.

Technical Risks:

- **AI Model Failure:** To ensure uninterrupted operation, maintain backup algorithms and manual override options up to date.
- **Data Breach:** Create an incident response strategy to quickly handle and report breaches.

Operational Risks:

- **Integration Failures:** To reduce interruptions, include stand-alone features or other integration techniques.
- **Low User Adoption:** To increase engagement, create user feedback loops and customised marketing efforts.

Economic Risks:

- **Budget Overruns:** Prioritise features and set aside money for unforeseen expenses.