Risk Matrix and Mitigation Plan

1. Mitigation Strategies for High-Priority Risks

The following table includes mitigation strategies proposed for high-priority risks identified in the project Risk Register. These strategies aim to reduce the likelihood and/or impact of the risks, thereby improving project resilience.

Risk ID: R001
Description: Manual scheduling process causes delays and errors.
Likelihood: High
Impact: High
Severity: Critical
Mitigation Strategy: Implement an automated scheduling platform with real-time conflict checks.

Risk ID: R002
Description: Staff resistance to new digital tools.
Likelihood: Medium
Impact: High
Severity: High
Mitigation Strategy: Provide mandatory training, assign departmental champions, and schedule regular feedback sessions.

Risk ID: R003
Description: Patient data breach due to poor cybersecurity.
Likelihood: Medium
Impact: High
Severity: High
Mitigation Strategy: Conduct regular data security audits, enforce encryption protocols, and implement multi-factor authentication.

Risk ID: R004
Description: System downtime during peak hours.
Likelihood: Medium
Impact: Medium
Severity: Medium
Mitigation Strategy: Set up system redundancy, conduct routine maintenance, and prepare quick-recovery support scripts

.

Risk ID: R005
Description: Inconsistent resource utilization across departments.
Likelihood: High
Impact: Medium
Severity: Medium
Mitigation Strategy: Deploy a centralized resource management dashboard to track and balance usage in real-time.

Risk ID: R006
Description: Budget overruns due to underestimation of system costs.
Likelihood: Low
Impact: Medium
Severity: Medium
Mitigation Strategy: Maintain contingency budget, conduct quarterly budget reviews, and implement budget tracking tools.

Risk ID	Risk description	Risk Category	Likelihood	Impact	Severity	Mitigation Strategy
R001	Manual scheduling process causes delays and errors	Operational	High	High	Critical Risk	Implement automated scheduling system
R002	Staff resistance to new digital tools	Stakeholder	Medium	High	High-priority Issue	Conduct training and change management sessions
R003	Patient data breach due to poor cybersecurity	Technical	Medium	High	High-priority Issue	Conduct regular data audits and improve encryption
R004	System downtime during peak hours	Technical	Medium	Medium	Mitigation Required	Establish redundancy and support for downtime recovery
R005	Inconsistent resource utilization across departments	Operational	High	Medium	Mitigation Required	Use a centralized resource tracking dashboard
R006	Budget overruns due to underestimation of system costs	Financial	Low	Medium	Monitor Closely	Conduct detailed financial planning and maintain contingency reserve

2. Contingency Plans

These contingency plans are designed to manage the high-priority risks in case they materialize despite mitigation efforts. Each plan includes immediate actions to contain the risk, minimize disruption, and recover project timelines.

Risk ID: R001
Contingency Plan: Shift to manual paper-based scheduling temporarily, increase admin staff coverage during high-volume periods, and notify patients of delays.

Risk ID: R002
Contingency Plan: If resistance continues, introduce change champions within departments, extend training duration, and provide one-on-one support sessions.

Risk ID: R003
Contingency Plan: Immediately isolate affected systems, notify IT security team, conduct root cause analysis, and communicate breach resolution to stakeholders.

Risk ID: R004
Contingency Plan: Switch to backup systems, notify stakeholders of delay, and activate emergency IT support to restore operations.

Risk ID: R005
Contingency Plan: Temporarily reassign staff and equipment from low-load to high-load departments and alert department heads to adjust workflows.

Risk ID: R006
Contingency Plan: Reallocate resources from non-critical areas, escalate to project finance team, and delay optional features if required to control budget.

Risk ID	Contingency Plan
R001	Shift to manual paper-based scheduling temporarily, increase admin staff coverage during high-volume periods, and notify patients of delays.
R002	If resistance continues, introduce change champions within departments, extend training duration, and provide one-on-one support sessions
R003	Immediately isolate affected systems, notify IT security team, conduct root cause analysis, and communicate breach resolution to stakeholders
R004	Switch to backup systems, notify stakeholders of delay, and activate emergency IT support to restore operations.
R005	Temporarily reassign staff and equipment from low-load to high-load departments and alert department heads to adjust workflows
R006	Reallocate resources from non-critical areas, escalate to project finance team, and delay optional features if required to control budget

3. Conclusion

By integrating proactive mitigation strategies and clear contingency plans, the HealthFirst Care project ensures preparedness against key operational risks. This approach enables timely responses to disruptions, maintains stakeholder confidence, and supports overall project success.