Project Name: Patient Management System

Date: 4/10/2023

Risk Register ID: PMS_R0

Project Manager: Vishal Yadav

Risk Identification

Risk ID	Risk Description	Risk Category	Risk Source
PMS_R01	Inadequate Security Measures	Security	External threats, unauthorized access
PMS_R02	System Compatibility Issues	Technical	Incompatibility with existing infrastructure
PMS_R03	Data Loss or Corruption	Operational	System failures, power outages, human errors
PMS_R04	Insufficient User Training	Human Factors	Lack of adequate staff training
PMS_R05	Vendor Dependency	External	Reliance on third-party vendors
PMS_R06	Scope Creep	Project Management	Uncontrolled project scope expansion
PMS_R07	Inadequate Backup and Recovery Procedures	Operational	Lack of robust backup and recovery plans

Risk Analysis

Risk ID	Impact	Likelihood	Severity	Priority
PMS_R01	4	3	4	High
PMS_R02	3	1	3	Medium
PMS_R03	4	3	4	High
PMS_R04	3	3	3	Medium
PMS_R05	4	3	4	High
PMS_R06	4	3	4	High
PMS_R07	4	1	3	Medium

Risk Response Planning

Risk ID	Risk Response Strategy	Responsible Party	Target Completion Date	Status
PMS_R01	Mitigation	IT Security Team	September 12, 2023	Open
PMS_R02	Mitigation	Development Team	September 15, 2023	Open
PMS_R03	Mitigation	IT Operations Team	September 18, 2023	Open
PMS_R04	Mitigation	Training Coordinator	September 20, 2023	Open
PMS_R05	Mitigation	Vendor Management Team	September 25, 2023	Open
PMS_R06	Avoidance	Project Manager	September 28, 2023	Open
PMS_R07	Acceptance	Project Manager	September 30, 2023	Open

Risk Monitoring and Control

Risk ID	Status Update	Date of Status Update	Key Performance Indicators (KPIs)
PMS_R01	No Change in Likelihood	October 1, 2023	No significant change in detected security incidents.
PMS_R02	Increase in Likelihood	October 2, 2023	System compatibility achieved has increased.
PMS_R03	No Change in Impact	October 4, 2023	Frequency of data backups and recovery time remain stable.
PMS_R04	No Change in Likelihood	October 3, 2023	Training completion rates and user feedback are consistent.
PMS_R05	No Change in Likelihood	October 7, 2023	Time taken to activate contingency plans and vendor communication effectiveness remain consistent.
PMS_R06	Increase in Impact	October 10, 2023	Increase in the number of requested scope changes and percentage of approved changes.
PMS_R07	No Change in Likelihood	October 5, 2023	The number of identified scope changes and impact assessment of accepted changes remain stable.

Contingency Planning

Risk ID	Contingency Plan Description	Trigger Points for Activation
PMS_R01	Enhanced monitoring and response procedures in case of security breaches	Significant increase in the number of detected security incidents.
PMS_R02	Expedited resolution plan for identified system compatibility issues.	Critical issues detected during system compatibility testing.
PMS_R03	Immediate implementation of backup procedures and expedited recovery.	Data backup failure or extended downtime during recovery.
PMS_R04	Rapid adjustment of training delivery methods or additional sessions.	Sharp decline in training completion rates or negative feedback.
PMS_R05	Activate alternative communication channels and vendor escalation plan.	Extended disruption in vendor communication or service delivery.
PMS_R06	Emergency review and approval process for scope changes.	Overwhelming increase in the number of scope change requests.
PMS_R07	Accelerated impact assessment and communication plan for scope changes	Identification of critical scope changes requiring immediate attention.