

Risk ID	Risk Description	Likelihood	Impact	Severity	Mitigation Strategy	Contingency Plan
R1	Resistance from senior staff to adopt new systems	High	Medium	High	Conduct training sessions and regular feedback meetings	If resistance persists, engage department champions and provide additional 1:1 coaching
R2	System downtime exceeding 1 hour/month	Medium	High	High	Implement failover systems and monitor uptime continuously	Switch to backup servers, notify affected departments, and implement hotfix protocol
R3	Data breaches compromising patient confidentiality	Low	High	Medium	Conduct regular data security audits and enforce encryption protocols	Isolate affected systems, notify IT/security, initiate root cause analysis, and inform stakeholders
R4	Delays in IT integration with legacy systems	High	Medium	High	Allocate buffer time and perform pre-deployment integration testing	Reassign resources to expedite integration, escalate to vendor support, and adjust deployment schedule
R6	Manual processes leading to resource bottlenecks	High	High	High	Automate key workflows and cross-train staff for critical roles	Temporarily reassign staff and extend service hours to handle peak demand