HealthFirst Care Risk Matrix and Mitigation Plan

Capstone Project M05L02

Adwoa Boama Acheampong | IBM Business Analyst learning project

Priority and planning basis

R01 and R02 have the maximum initial score of 9. R04, R06 and R07 score 6 and are also High on the 3 × 3 planning matrix. These five high-priority risks require prevention, trigger, owner and contingency; the remaining five are monitored with the same fields. No residual reduction is claimed until controls are tested and owners rescore each risk.

Updated 3 × 3 priority matrix

3 × 3 likelihood–impact matrix

Scores = likelihood × impact; all ten risks shown by stable ID

Likelihood ↓			
3	Score 3: No listed risk	Score 6: R06	Score 9: R01, R02
2	Score 2: No listed risk	Score 4: R03, R05, R08, R09	Score 6: R04, R07
1	Score 1: No listed risk	Score 2: R10	Score 3: No listed risk

Low 1–2 · Medium 3–4 · High 6–9; initial planning scores, not observed residual risk.

Impact → 1 Low · 2 Medium · 3 High

Initial positions are shared with the risk register. After evidence-based mitigation, owners update likelihood and impact in the workbook; the matrix recalculates from those inputs.

ID	Preventive action	Owner	Trigger	Contingency	Residual target	Review
R01	Conflict rules, scenario UAT and daily exception review	Operations manager	Double booking or override trend	Pause affected scheduling path; use controlled manual calendar and reconcile later.	Unscored; review after test	Daily during pilot
R02	Field mapping, reconciliation, retry queue, monitoring and rollback	IT manager	Stale sync or reconciliation variance	Disable failing interface; use validated batch extract and preserve exception log.	Unscored; review after test	Daily during pilot
R03	Department thresholds, protected capacity and escalation	Clinical operations	Wait or utilisation threshold breach	Rebalance slots/resources or invoke approved surge, transfer or reschedule rules.	Unscored; review after test	At each stage gate

ID	Preventive action	Owner	Trigger	Contingency	Residual target	Review
R04	Least privilege, MFA, audit logging, encryption and incident exercises	Security lead	Unauthorized access or delivery exposure	Contain access, preserve evidence and invoke the approved privacy incident process.	Unscored; review after test	Daily during pilot
R05	Co-design, role training, floor support and usage review	Change lead	Bypass or duplicate-entry trend	Remove unsafe parallel process, deploy champions and target retraining.	Unscored; review after test	At each stage gate
R06	Validation rules, exception queue, ownership and quality scorecard	Data owner	Missing or duplicate keys rise	Qualify affected KPI, quarantine suspect rows and correct the source before decision use.	Unscored; review after test	Daily during pilot
R07	Downtime procedure, monitoring and reconciliation drills	IT incident lead	Connectivity or service outage	Use the approved downtime list and reconcile every record after restoration.	Unscored; review after test	Daily during pilot
R08	Accessibility review, assisted booking and usability testing	Patient experience lead	Abandonment or support complaints	Switch to assisted booking or check-in and correct inaccessible content.	Unscored; review after test	At each stage gate
R09	Metric dictionary, denominator review and formal baseline approval	Project sponsor	Conflicting dashboard interpretations	Suspend the disputed KPI from decision use until definition and baseline are approved.	Unscored; review after test	At each stage gate
R10	Scope baseline, change assessment and sponsor decision	Project manager	Unplanned deliverable or dependency	Stop unapproved work and route the change through sponsor review.	Unscored; review after test	At each stage gate

Escalation and continuity

Event	Immediate action	Continuity method	Decision owner
Scheduling or HIS outage	Declare incident and preserve current queue	Controlled downtime list with reconciliation	IT incident lead
Incorrect or missing feed	Quarantine affected dashboard data	Show freshness warning and use validated prior extract	Data owner
Notification failure or exposure	Stop repeated sends and assess recipients	Phone high-risk changes using minimum necessary data	Operations and security
Capacity threshold breach	Escalate and reassess appointments	Approved overflow, transfer or reschedule rule	Clinical lead
Critical security event	Revoke access, contain and preserve evidence	Approved minimum-data manual process	Security lead

Acceptance evidence

- Control owner is named and accepts responsibility.
- Trigger can be observed from an agreed source.
- Preventive control passes its planned test.
- Contingency is exercised or walkthrough evidence is retained.
- Residual score and any remaining limitation are reviewed by the sponsor.

Conclusion

The mitigation plan is complete as a planning artifact. It does not claim that controls have been implemented, tested or accepted. Those statuses remain open in the RTM and risk register until evidence is added.