

Week 6. Creating a Contingency Plan

Healthcare Management System (MediCare Solutions)

Janki Patel	2520611
Nirav Thummar	2537379
Sameer Sukhadiya	253660

Contingency Plan – MediCare Solutions Healthcare Management System

1. Introduction

MediCare Solutions relies on an integrated Electronic Health Records (EHR) system to store and manage patient medical histories, lab results, prescriptions, appointments, and treatment plans. Because healthcare operations depend heavily on continuous access to accurate patient data, a contingency plan is essential to ensure service continuity during disruptions.

2. Data Classification Scheme (Required Learning Objective)

Data Categories

- **Confidential (Highest Sensitivity)**
 - Patient medical histories
 - Lab results
 - Prescriptions
 - Treatment plans
 - Personally identifiable information (PII)
 - Insurance and billing information
- **Internal Use**
 - Staff schedules
 - Internal policies
 - Operational workflows
- **Public**
 - Marketing materials
 - Public health announcements

Classification Controls

- Encryption (AES-256) for confidential data
- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Audit logging and monitoring

3. Risk Assessment Methodology (Required Learning Objective)

Selected Methodology: NIST SP 800-30

Chosen because it is widely used in healthcare, aligns with HIPAA/GDPR principles, and provides structured steps:

1. **Identify threats**
2. **Identify vulnerabilities**
3. **Determine likelihood**
4. **Determine impact**

5. **Calculate risk rating**
6. **Recommend controls**

Key Threats

- Ransomware attacks
- EHR system failure
- Insider misuse
- Network outage
- Natural disasters
- Third-party vendor failure

4. Gap Analysis Plan (Required Learning Objective)

Current State vs. Desired State

Area	Current State	Desired State	Gap	Action
Data Backup	Daily backups	Real-time replication	Medium	Implement cloud-based failover
Access Control	Password-only	MFA + RBAC	High	Deploy MFA system
Incident Response	Basic procedures	Full IR team + playbooks	High	Create IR team & training
System Hardening	Standard configs	CIS benchmarks	Medium	Apply CIS hardening

5. Risk, Threat & Vulnerability Assessment

Threats

- Malware infections
- Unauthorized access
- Power failure
- System misconfiguration
- Human error

Vulnerabilities

- Outdated software
- Weak passwords
- Single network provider
- Lack of offline patient data access
- Insufficient staff training

Risk Outcomes

- Loss of patient data
- Delayed treatment
- Legal penalties
- Reputational damage
- Financial loss

6. Malware Attack & Confidential Data Exposure Outcomes

Potential Impacts

- Encryption of EHR database (ransomware)
- Theft of patient medical records
- Manipulation of lab results or prescriptions
- Service downtime affecting emergency care
- Regulatory fines (GDPR, ICO reporting within 72 hours)

Mitigation

- Endpoint protection
- Network segmentation
- Regular patching
- Staff phishing training
- Immutable backups

7. Security Countermeasures

Technical Controls

- Firewalls, IDS/IPS
- MFA and RBAC
- Database encryption
- Secure VPN for remote access
- Automated patch management

Administrative Controls

- Security policies
- Staff training
- Vendor risk management
- Incident response procedures

Physical Controls

- CCTV
- Access badges
- Secure server rooms
- Environmental controls (fire suppression, cooling)

8. System Hardening Purposes

- Reduce attack surface
- Prevent unauthorized access
- Ensure system stability
- Protect sensitive healthcare data
- Improve compliance with healthcare regulations

Hardening Activities

- Disable unused services
- Apply CIS benchmarks
- Enforce strong password policies
- Patch OS and applications
- Enable logging and monitoring

9. Contingency Plan (Core Deliverable)

A. Objectives

- Maintain continuity of patient care
- Protect patient data integrity
- Restore systems quickly after disruption
- Ensure compliance with healthcare regulations

B. Contingency Triggers

- EHR system outage
- Cyberattack
- Network failure
- Power outage
- Natural disaster
- Staff shortage

C. Response Procedures

1. EHR System Failure

- Switch to paper-based documentation
- Access offline patient data snapshots
- IT initiates system recovery
- Notify clinical staff

2. Cybersecurity Incident

- Isolate affected systems
- Activate Incident Response Team

- Switch critical operations to offline mode
- Notify regulatory authorities
- Conduct forensic investigation

3. Network or Power Outage

- Activate backup generators
- Switch to secondary ISP
- Use offline patient data access

4. Natural Disaster

- Evacuate patients if needed
- Move operations to secondary site
- Protect physical records and servers

5. Staff Shortage

- Activate cross-trained backup staff
- Enable remote work for admin teams
- Prioritize emergency care

D. Backup & Recovery

- Daily encrypted backups
- Offsite cloud replication
- Weekly recovery testing
- RTO: 2–4 hours
- RPO: 24 hours

E. Communication Plan

- Internal alerts (SMS, email, PA system)
- Patient notifications for delays
- Regulatory notifications
- Staff briefings

F. Roles & Responsibilities

- **Contingency Manager:** Activates plan
- **IT Team:** System recovery
- **Clinical Staff:** Manual workflows
- **Admin Team:** Communication & scheduling
- **Compliance Officer:** Regulatory adherence

G. Testing & Maintenance

- Quarterly drills
- Annual plan review
- Update after major incidents
- Staff training refreshers

H. Post-Incident Review

- Root-cause analysis
- Lessons learned
- Update policies
- Report to leadership

10. Business Success Alignment

A strong contingency plan ensures:

- Continuous patient care
- Reduced downtime
- Regulatory compliance
- Protection of reputation
- Operational resilience
- Improved trust from patients and partners