

Healthcare IT Continuity & Disaster Recovery

Prepared by Dr. Hesham Mousli

MHA621
Healthcare Informatics

Lecture 9



Intended Objectives

1. **Examine** the continuity life cycle and its role in healthcare IT.
2. **Evaluate** the importance of continuity planning, including disaster recovery.
3. **Explain** the rationale and key steps in developing a Business Continuity Plan (BCP).
4. **Identify** threats to business operations and information systems.
5. **Review** legal, accreditation, and compliance requirements for continuity planning.

Overview

Chapter

09

➤ Why Continuity Planning Matters in Healthcare IT ?

1. Healthcare depends on **24/7 data access** (EHRs, labs, imaging) for patient care.
2. **System downtime** leads to **delayed care, financial loss, and reputational damage.**
3. Regulations (HIPAA, TJC, PAHPA) mandate **Business Continuity Plans (BCPs).**

Key Threats to Healthcare IT



Key Threats to Healthcare IT

- 1. Natural Disasters:** Events like hurricanes, floods, earthquakes, and wildfires can disrupt healthcare IT infrastructure, causing system outages and data loss.
- 2. Cyber Threats:** Cyberattacks, including ransomware and data breaches, compromise patient information, disrupt operations, and demand costly recovery efforts.
- 3. Insider Threats:** Unauthorized access, employee negligence, or intentional misuse of IT systems can lead to data leaks or operational failures.

Key Threats to Healthcare IT

4. **Equipment Failures:** Hardware malfunctions, power outages, or software crashes can interrupt patient care and system functionality.
5. **Data Integrity Risks:** Corruption, accidental deletion, or failure to back up critical healthcare data can impact clinical decision-making and compliance.

Continuity Planning Process

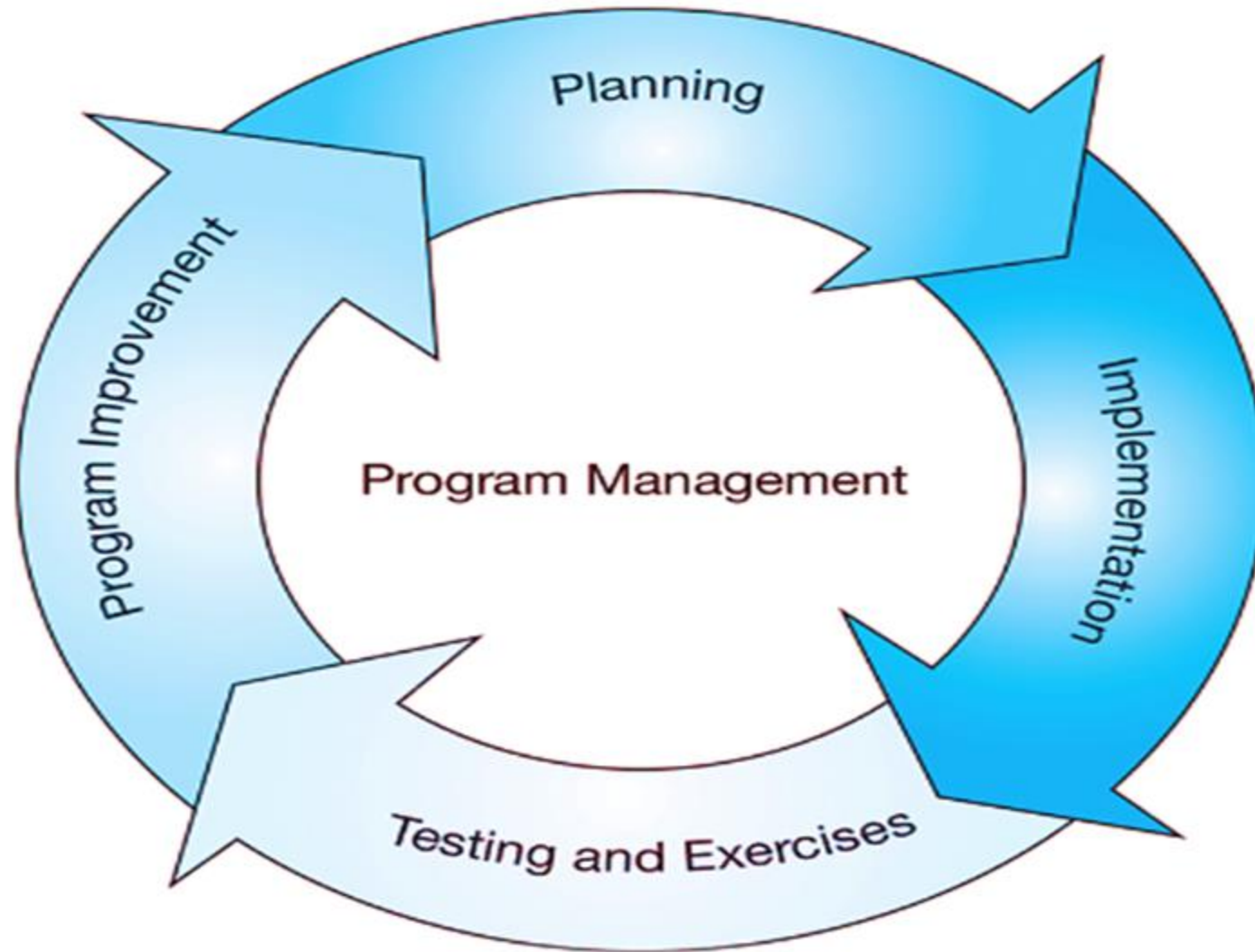


What Is Continuity Planning?

- Continuity planning , usually called business-continuity planning (**BCP**) , is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.



Preparedness Program Planning Stages



Continuity Planning Process

1. Continuity Program Management :

- **Leadership Commitment:** Assign a Business Continuity Plan (BCP) Coordinator (e.g., IT Director + Clinical Lead).
- **Budgeting:** Allocate funds for backups, cloud storage, and drills.
- **Policy Development:** Define roles (e.g., "Who declares a disaster?").

Continuity Planning Process

2. Planning:

➤ **Risk Assessment:** Threat and Hazard Identification and Risk Assessment (**THIRA**) **Method:**

- A. **Identify Threats:** (e.g., ransomware, power outage).
- B. **Determine Vulnerabilities:** (e.g., single data center).
- C. **Estimate Impact:** (e.g., EHR downtime = delayed surgeries).
- D. **Prioritize Risks:** (e.g., cyberattacks > natural disasters).

Continuity Planning Process

➤ Business Impact Analysis (BIA)

- A. **Business Impact Analysis (BIA)** is a structured process to evaluate the potential impact of disruptions on hospital operations. It helps prioritize recovery efforts by identifying critical functions, assessing downtime tolerance, and setting **Recovery Time Objectives (RTOs)**.
- B. **Recovery Time Objective (RTO)** is the maximum acceptable downtime for a hospital system or function after a disruption before it causes significant operational, financial, or patient safety risks. It defines the target time to restore services to an acceptable level.

Continuity Planning Process

➤ Business Impact Analysis (BIA) steps:

1. **Survey Managers:** Interview department heads (e.g., "How long can billing operate offline?").
2. **Identify Critical Functions:**
 - I. **Clinical:** EHRs, lab systems.
 - II. **Administrative:** Payroll, supply chain.
3. **Rank by Recovery Time Objective (RTO).**

Continuity Planning Process

➤ Ranking by Recovery Time Objective (RTO):

Category	Recovery Time Objective (RTO)	Examples
1. Critical	< 12 hours	ICU monitoring, pharmacy orders
2. Vital	12–24 hours	Radiology scheduling
3. Important	1–3 days	HR onboarding

4. **Document Dependencies:** "Lab system outage delays radiology reports."

3. Implementation:

- A. **Emergency Response Plan (ERP):** Evacuation, lockdown procedures.
- B. **Crisis Communication Plan (CCP):** Spokesperson, alert systems.
- C. **IT Disaster Recovery Plan (ITP):** Data restoration steps.

Continuity Planning Process

3. Implementation:

A. Emergency Response Plan (ERP):

- **System Failure Response:** Protocols for responding to EHR outages, cybersecurity attacks, or data center failures.
- **Evacuation of Digital Operations:** Transition to backup servers or offline documentation methods to maintain patient care.
- **Lockdown Procedures:** Restrict access to compromised IT systems, disable affected networks, and secure critical databases to prevent further breaches.

3. Implementation:

B. Crisis Communication Plan (CCP):

- **Designated IT Spokesperson:** A trained IT or hospital representative to communicate system status, recovery timelines, and mitigation measures.
- **Alert & Notification Systems:** Automated alerts notify staff of system failures, cybersecurity threats, and alternative workflows via SMS, intranet, and emergency emails.
- **Stakeholder Coordination:** Clear communication with leadership, vendors, and regulatory bodies (e.g., Ministry of Health, cybersecurity teams) to ensure compliance and rapid resolution.

4. Testing & Exercises:

A. Tabletop Drills (Scenario-Based Exercises):

- Simulate a ransomware attack or EHR downtime to assess response readiness.
- **Example:** “How do we switch to paper records if the system is locked?”
- Ensures staff know alternative workflows and IT teams can contain threats efficiently.

4. Testing & Exercises:

B. Full-Scale Mock Disasters (Real-World Testing):

- **Test backup generators** to verify power redundancy for IT systems.
- **Simulate cloud failover** to confirm seamless switching to secondary data centers.
- **Help identify weaknesses** in system resilience and ensure minimal disruption to patient care.

Backup & Recovery Strategies



1. Backup Methods

Method	Pros	Cons	Best For
Tape Backup	Low cost, long-term storage	Slow recovery, physical transport	Archives (e.g., old records)
Cloud Backup	Automated, scalable	Requires bandwidth	EHRs, real-time data
Data Mirroring	Zero downtime	Expensive	Critical systems (e.g., ICU)

2. Recovery Strategies

Recovery Strategy	Description	Pros	Cons	Best For
Hot Site	A fully operational backup facility with real-time data replication.	Immediate failover (minimal downtime) Fully configured with servers & software.	Expensive (high maintenance cost) Requires constant updates.	Critical systems (ICU monitoring, EHRs).
Cold Site	A facility with power and networking but without pre-installed servers or software.	- Lower cost than Hot Site. - Available for long-term recovery.	Slower recovery (requires setup) Not suitable for real-time needs.	Non-urgent systems (HR, finance).
Electronic Vaulting	Automatic, secure off-site backups of critical data (e.g., patient records, EHRs).	- Automated & reduces human error. - HIPAA-compliant & secure.	- Depends on internet bandwidth. - Recovery speed varies.	Protecting patient data from loss or cyberattacks.

5. Program Improvement:

A. Post-Drill Reviews (Evaluating Effectiveness):

- **Definition:** A structured assessment after a disaster recovery drill or real incident.
- **Purpose:** Identifies successes, failures, and gaps in the recovery process.

5. Program Improvement:

A. Post-Drill Reviews (Evaluating Effectiveness):

➤ Key Questions to Ask:

- **RTO Compliance:** Was EHR recovery within the set timeframe (e.g., 4 hours)?
- **System Restoration:** Were all critical systems (e.g., pharmacy orders, ICU monitoring) fully restored?
- **Staff Readiness:** Did IT, clinicians, and admin teams follow their assigned roles?
- **Communication Efficiency:** Did emergency alerts and escalation procedures work as expected?

5. Program Improvement:

B. Corrective Actions (Enhancing Disaster Readiness)

- **Definition:** Improvements based on **post-drill findings** to strengthen future response.
- **Examples of Corrective Actions:**
 - **Update Contacts:** Keep IT, clinical, and admin emergency lists current.
 - **Patch Security Gaps:** Fix software, network, and backup vulnerabilities.
 - **Revise Disaster Recovery Plan (DRP):** Adapt protocols based on drill findings.
 - **Train Staff:** Address skill gaps for better response.
 - **Improve Backups:** Optimize cloud settings and test failovers regularly.

Mock Scenario Example



➤ **Incident Simulation:**

A ransomware attack locks hospital systems, demanding payment to restore access.



➤ What is Ransomware?

- **Ransomware** is a type of **malware** (malicious software) that **encrypts files or locks systems**, demanding a **ransom payment** to restore access.

➤ How It Affects Healthcare IT?

- Blocks access to **EHRs, lab systems, and pharmacy orders**.
- Causes **patient care delays** and financial losses.
- Poses **data breach risks** (violating HIPAA and other regulations).

➤ Response Steps:

■ IT Security Team:

- Detects and isolates infected servers to prevent the virus from spreading.
- Activates **cybersecurity protocols** and notifies leadership.

■ EHR Recovery Team:

- Switches operations to **cloud-based backup EHRs**.
- Ensures **critical systems (ICU, pharmacy, radiology)** are restored first.

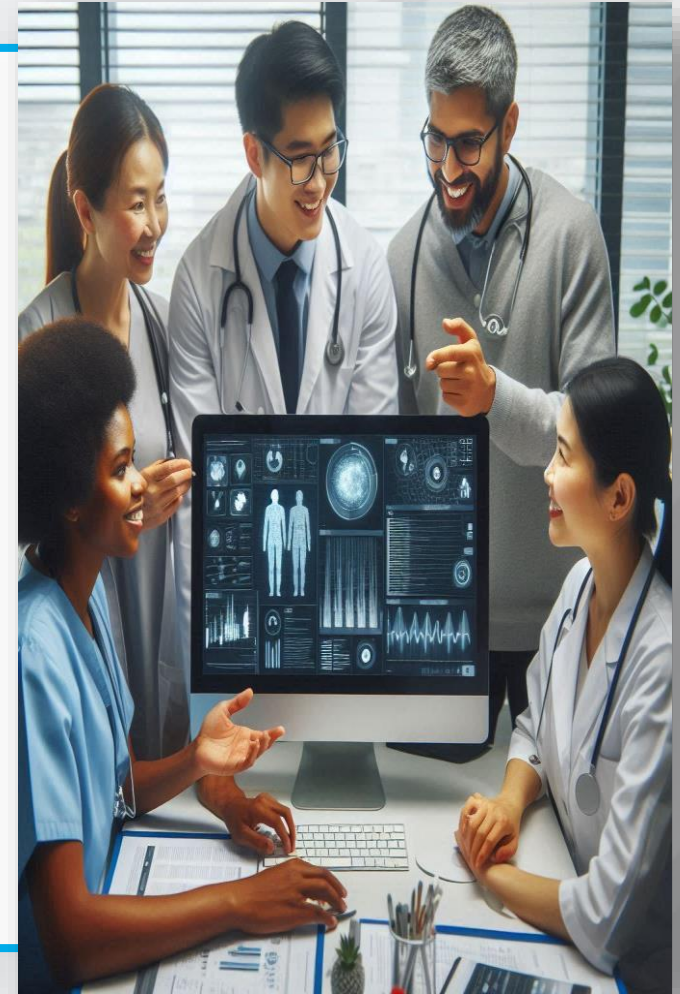
■ Communication Team:

- Alerts **hospital staff** via emergency channels.
- Notifies **patients and stakeholders** about service disruptions.

➤ Post-Test Review:

- **Issue Identified:** Backup restoration **took 6 hours**, exceeding the **4-hour Recovery Time Objective (RTO)**.
- **Action Plan:**
 - **Upgrade bandwidth** for faster cloud recovery.
 - **Increase the frequency of backup testing** to improve response time.
 - **Train staff on ransomware response drills** for faster coordination.

Common Pitfalls & How to Avoid Them



➤ **Pitfall:** No BIA Done → Don't Know Which Systems Are Critical

- **Problem:** Without a **Business Impact Analysis (BIA)**, you can't identify which systems are essential for patient care and hospital operations.
- **Solution:**
 - Conduct a **BIA** before purchasing backup solutions.
 - Identify **critical systems** (e.g., EHRs, ICU monitoring) and their recovery priorities.

➤ **Pitfall: Backups Never Tested → Fail When Needed**

- **Problem:** Backups that aren't regularly tested may fail during a disaster, delaying recovery.
- **Solution:**
 - Perform **quarterly restore tests** to ensure data integrity.
 - **Simulate recovery** of a sample system (e.g., EHRs) during drills to validate backup effectiveness.

Key Recommendations

- **Start Small:** Focus on “**Category 1 systems**” first (EHRs, labs).
- **Automate:** Use tools like “**Veeam for Healthcare**”, a data backup and recovery software solution.
- **Train:** Annual drills for “**IT + clinical staff**” (e.g., "How to access backup EHRs?").
- **Document:** Maintain logs of backup tests for “**Survey Audit Compliance**”.

1. **Healthcare IT** must ensure **24/7 system availability** to prevent care delays, financial loss, and compliance violations.
2. **Major threats** include natural disasters, cyberattacks, equipment failures, and data corruption.
3. **A structured BCP** requires risk assessment, BIA, and clear RTOs for critical functions like EHRs and labs.
4. **Effective implementation** involves emergency response plans, IT recovery protocols, and crisis communication strategies.

5. **Regular testing** (tabletop drills, mock disasters) ensures staff readiness and system resilience.
6. **Automated backups**, cloud failover, and quarterly recovery tests are essential for reliable data restoration.
7. **Post-drill reviews** identify gaps in **RTO** compliance, communication, and system recovery for continuous improvement.
8. **Avoid failures** by prioritizing BIA, testing backups, and training staff annually on disaster response.



Thank You