# CYBERSECURITY INCIDENT RESPONSE PLAN

Submitted by: Ankit Pradhan

Course: IT Security: Ethical and Legal Issues

Section: A

Date: October 23, 2025

Professor: Ionut Anghelache

Company: MediHealth

## HOW/WHEN TO USE THE INCIDENT RESPONSE PLAN

The MediHealth Systems Incident Response Plan (IRP) is activated upon detection or suspected occurrence of a cybersecurity incident affecting any critical system or protected health information (PHI). Incidents that require plan activation include data breaches, ransomware infections, unauthorized system access, and network disruptions that compromise confidentiality, integrity, or availability. The plan ensures timely response aligned with both HIPAA requirements and NIST Cybersecurity Framework (CSF) functions: Identify, Protect, Detect, Respond, and Recover.

This plan should be implemented immediately once an anomaly is validated as a potential incident by the Security Operations Center (SOC) or IT department. Swift activation enables containment, preservation of evidence, mitigation of business disruption, and compliance with federal reporting regulations.

## EVENT HANDLING

Event handling follows the NIST SP 800-61 lifecycle of four stages—Preparation, Detection & Analysis, Containment & Eradication, and Post-Incident Activity.

Event Categories:

- *Unauthorized Access:* Breach of user or administrative credentials.
- *Malware/Ransomware:* System infection that encrypts or corrupts files.
- *Denial of Service :* Attack hindering access to healthcare applications.
- *Data Exfiltration:* Unauthorized transfer of PHI or financial data.
- *Insider Threat:* Malicious or accidental compromise by internal personnel.

Categorization and Prioritization:
Events are classified according to severity:

- High (Critical systems affected, PHI exposed)
- Medium (Limited functional disruption)
- Low (Minor alert, monitored for escalation)

Each event is logged in an Incident Event Log, including timestamps, actions taken, and responsible personnel.

## INCIDENT RESPONSE TEAM

The MediHealth Incident Response Team (IRT) operates under the Chief Information Security Officer (CISO). The composition includes:

| Role | Responsibility |
|---|---|
| CISO | IRP oversight, regulatory reporting |
| IT Security Manager | Coordinates technical investigation, containment |
| Systems Administrator | Manages isolation and recovery processes |
| Legal & Compliance Officer | Ensures HIPAA and breach notification compliance |
| Public Relations Officer | Communicates externally with media and stakeholders |
| HR Representative | Addresses employee-related incidents |
| Forensic Analyst | Conducts post-incident evidence collection and analysis |

All members undergo recurring NIST-aligned training and simulated attack drills to maintain readiness.

## RESPONSE

Incident response follows structured processes based on NIST functions:

1. Preparation:

- Maintain updated network diagrams and asset inventories.
- Implement endpoint protection and regular employee training.

2. Detection and Analysis:

- Utilize automated intrusion detection (IDS) and Security Information and Event Management (SIEM) systems to monitor and flag irregularities.
- Analyze logs for malicious patterns (login anomalies, exfiltration).

3. Containment, Eradication, and Recovery:

- Containment: To stop the lateral spread over the system, the infected systems will be isolated as soon as possible.
- Eradication: Remove malware, patch vulnerabilities, reset credentials.
- Recovery: Gradually reintroduce systems into operation after validation and verification of clean backups.

4. Post-Incident Review:

- Conduct a “lessons learned” session and produce a Post-Incident Report.
- Update the IRP to address newly identified weaknesses.

Specific Asset Plans:

- Electronic Health Records (EHR): In EHR records, data is encrypted with multifactor authentication required for accessing the data.
- Network Hardware: Redundant failover equipment provisioned.
- Workstations: Remote wipe capability activated via endpoint management.
- Cloud Services: Contractual SLAs ensure rapid recovery and data integrity.

Checklists and notification triggers include internal alerts to executive leadership and mandatory regulatory reporting to HHS OCR under HIPAA in case of PHI exposure.

## IMPACTS ON THE ORGANIZATION

A recent ransomware simulation estimated that downtime of EHR systems would cost MediHealth approximately $250,000 per day in delayed care and patient compensation. Additional impacts include:

- Financial: Recovery tooling, legal fees, and potential federal penalties.
- Reputational: Diminished trust among patients and partners.
- Regulatory: Required reporting to HHS and state authorities within breach notification timelines.

Mitigating these impacts underscores the necessity of testing and refining incident protocols continuously.

## CONCLUSION

An effective incident response plan enables MediHealth Systems to act decisively and legally during cybersecurity incidents. Continuous improvement, simulation exercises, and adherence to

NIST SP 800-61 Rev. 3 guide the organization toward resilience, minimizing operational disruption, and maintaining public confidence.

## INFORMATION SOURCES

- NIST SP 800-61 Rev. 3: *Computer Security Incident Handling Guide*
- Hyperproof: *Cybersecurity Incident Response Plan Checklist*
- HSCC: *Coordinated Healthcare Incident Response Plan (CHIRP)*
- BlueVoyant: *Top 8 Incident Response Plan Templates*