Incident Detection and Response Policy

Prepared by: Rameen Mughal
Date: November 13, 2025

Industry: Pharmaceuticals
Policy Owner: Information Security Department
Effective Date: November 13, 2025
Review Cycle: Annually

I. Pharmaceuticals Industry Overview

The pharmaceuticals industry focuses on the research, development, production, and distribution of medicines that improve and sustain human health. It plays a vital role in public health by creating drugs and vaccines used to prevent, treat, and manage diseases.

This industry involves complex processes such as clinical trials, drug formulation, regulatory approvals, and manufacturing, all of which require the highest standards of data accuracy, security, and compliance.

Pharmaceutical organizations handle highly sensitive information, including:

1. **Clinical trial data** involving patient participants.
2. **Research and intellectual property (IP)** related to new drug compounds.
3. **Confidential health records** and regulatory documentation.

II. Purpose

The purpose of this policy is to establish a structured approach for identifying, responding to, managing, and recovering from information security incidents that could affect the confidentiality, integrity, or availability of clinical trial data, research intellectual property (IP), or patient records.

III. Scope

This policy applies to all employees, contractors, and third-party vendors who handle or have access to the organization’s information systems, networks, and sensitive data across all pharmaceutical research, production, and administrative operations.

IV. Roles and Responsibilities

Roles	Responsibilities
Information Security Team	Lead incident investigation, constraint, and coordination.
IT Operations	Support system restoration and technical mitigation.
Department Heads	Make sure staff follow the rules for reporting and escalating incidents.
Employees	Report incidents immediately and cooperate with investigations.
Legal & Compliance Team	Evaluate applicable regulatory requirements and ensure timely reporting to external authorities, such as HIPAA or GDPR, as necessary.

V. Policy Statements

The organization must maintain a proactive and coordinated Incident Response (IR) capability to ensure timely detection, containment, investigation, and resolution of all security incidents. All incidents must be reported immediately to the Information Security Team through approved channels.

1. **Incident Identification:**
    - All personnel must immediately report any detected or suspected security incident, such as unauthorized access, malware infection, data loss, or unusual system activity.
    - Reports should be submitted via the official Incident Reporting Form or through the Security Operations Center (SOC) hotline.

2. **Classification & Prioritization:**
   Incidents shall be classified by impact and urgency to ensure an appropriate response. Classification is determined based on the potential effect on clinical data integrity, patient privacy, research operations, or regulatory compliance.

   The Incident Response Lead determines final classification after initial triage.

Severity Level	Description
Critical	Major compromise of clinical trial data, research IP, or patient records with regulatory impact.
High	Significant disruption of systems or unauthorized access without confirmed data loss.
Medium	Limited system compromise or suspicious activity under investigation.
Low	Isolated and contained event with minimal risk.

3. **Containment & Eradication:**
   The IR team must immediately isolate affected systems from the network to prevent further spread. Malicious code or unauthorized access must be removed, and system configurations hardened before reconnection.

4. **Investigation & Analysis:**
   During an incident, the response team must carefully gather and preserve all relevant data that could help understand what happened. This includes **system logs**, **network activity records**, **emails,** and **snapshots** of affected devices or servers.

   All evidence should be collected using **forensic best practices** to ensure its accuracy and legal validity meaning no data should be altered or deleted during the process.

   The security team must then analyze the collected evidence to:
   - Identify how the incident occurred (the attack vector).
   - Determine which systems, data, or users were affected.
   - Assess the root cause, such as a software vulnerability or human error.
   - Evaluate whether the incident involves regulated information (e.g., patient data or research files).

   If any protected data (such as patient records under HIPAA or personal data under GDPR) was accessed, exposed, or lost, the organization must immediately notify regulatory authorities and affected parties as required by law.

5. **Recovery:**
   Restore affected systems and data from verified backups only after confirming they are free of compromise. System functionality must be validated and monitored for recurrence of abnormal activity.

6. **Post-Incident Review:**
   Within **five (5) business days** of incident closure, conduct a formal lessons-learned session to evaluate response effectiveness. Update security controls, playbooks, and employee training based on findings.

7. **Documentation:**
   Maintain detailed incident records including classification, timeline, actions taken, responsible personnel, and remediation outcomes. Documentation must be retained for a **minimum of three (3) years** for audit and compliance purposes.

VI. Enforcement

Failure to adhere to this policy may result in disciplinary action, up to and including termination, as well as potential legal consequences for non-compliance with applicable data protection regulations.

VII. Justification

In the pharmaceutical industry, security incidents can jeopardize clinical trial data integrity, delay regulatory approvals, and expose sensitive patient or research information.

A formal Incident Response Policy ensures rapid detection, effective containment, and regulatory compliance, minimizing damage to data, systems, and organizational reputation.

VIII. Exceptions

Any deviation from this Incident Response Policy must be formally approved in advance by the Information Security Department. Exceptions may be granted under specific circumstances, such as temporary operational needs or emergency situations, provided that:

- The risk is assessed and documented.
- Alternative controls or compensating measures are implemented to mitigate potential impact.
- Approval is obtained in writing and retained for audit purposes.