Data Leak Handling Process

Saudi Commission for Health Specialties (SCFHS)

Date: 01/12/2024

المملكة العربية السعودية
Kingdom of Saudi Arabia
ص.ب P.O.Box 94656
الرياض Riyadh 11614
ت. T. +966 11 290 5555
ف. F. +966 11 480 0800
info.scfhs.org.sa
www.scfhs.org.sa

1. Objective

To provide a structured and compliant approach for handling data leaks, ensuring mitigation of risks, safeguarding personal data, and maintaining compliance with SDAIA NDMO and PDPL.

2. Scope

This process applies to all systems, applications, and employees of the SCFHS that manage, process, or store personal data.

3. Process Steps

Step 1: Detection and Identification

1. **Proactive Monitoring**

    a. Implement automated monitoring tools like Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and Endpoint Detection & Response (EDR) systems to identify potential leaks in real time.
    b. Regularly conduct penetration testing and vulnerability scans.

2. **Incident Reporting**

    a. Establish a 24/7 incident reporting mechanism (e.g., hotline, email, or online portal) for employees, vendors, or third parties to report suspected data leaks.
    b. Employees must escalate incidents to the Data Protection Officer (DPO) immediately.

3. **Initial Classification**

    a. Categorize the data leak based on the severity, volume, and type of personal data involved:

        i. **Low**: Non-sensitive data with minimal impact.
        ii. **Medium**: Sensitive data affecting a small number of individuals.
        iii. **High**: Highly sensitive data or large-scale impact on Data Subjects.

Step 2: Immediate Containment

1. **Secure Affected Systems**

    a. Disconnect affected systems or devices from the network to prevent further data exposure.
    b. Suspend compromised user accounts or credentials.

2. **Limit Data Access**

    a. Restrict access to the leaked data to authorized personnel involved in the investigation.
    b. Temporarily disable public-facing systems or APIs if they are identified as sources of the leak.

3. **Preserve Evidence**

    a. Ensure that logs, email trails, and other artifacts related to the incident are preserved for investigation.

Step 3: Investigation and Analysis

1. **Form an Incident Response Team**

    a. Include representatives from IT Security, Legal, Compliance, and the DPO to manage the investigation.

2. **Identify Root Cause**

    a. Determine the origin and scope of the data leak:

        i. Was it caused by a human error, system failure, or cyberattack?
        ii. Which systems, processes, or vendors were involved?

3. **Impact Analysis**

    a. Assess the affected data types (e.g., personal identifiers, financial information, health records).
    b. Evaluate the potential harm to Data Subjects, such as identity theft or reputational damage.

4. **Document Findings**

    a. Record details such as the timeline of events, affected systems, and the scope of the leak.

Step 4: Notification to Stakeholders

1. **Internal Stakeholder Notification**

    a. Notify senior management, the Data Governance Organization (DGO), and the Board, as appropriate.

b. Provide an initial assessment of the leak and actions taken.

2. **Regulatory Notification**

   a. Notify the Supervisory Authority (e.g., SDAIA NDMO) within 72 hours of identifying a significant data leak.
   b. Include:

      i. Nature of the leak.
      ii. Data categories and affected individuals.
      iii. Steps taken to mitigate risks.
      iv. Point of contact (e.g., DPO).

3. **Data Subject Notification**

   a. Notify Data Subjects if the leak poses a high risk to their rights or freedoms.
   b. Provide:

      i. A description of the data leak.
      ii. Possible consequences.
      iii. Recommended actions (e.g., change passwords, monitor accounts).
      iv. Contact details for assistance (DPO or helpdesk).

Step 5: Mitigation and Recovery

1. **Implement Immediate Mitigation**

   a. Patch vulnerabilities, update software, and restore system integrity.
   b. Remove unauthorized access to leaked data from public platforms or servers.

2. **Data Recovery**

   a. Use secure backups to restore lost or corrupted data.

3. **Third-Party Coordination**

   a. If the leak involves third-party vendors, coordinate with them to ensure they address their vulnerabilities.

Step 6: Post-Incident Actions

1. **Root Cause Resolution**
    a. Address the root cause of the incident to prevent recurrence (e.g., implement stronger access controls, enhance network security).
2. **Employee Training**
    a. Provide targeted training to employees on avoiding similar incidents (e.g., phishing awareness, secure data handling).
3. **Policy Updates**
    a. Update data protection policies and procedures to reflect lessons learned.
4. **Communication**
    a. Share a summary of the incident and its resolution with internal teams to build awareness and enhance response readiness.

Step 7: Documentation and Compliance

1. **Incident Report**
    a. Prepare a detailed incident report including:
        i. Incident timeline.
        ii. Affected data types and scope.
        iii. Mitigation steps and outcomes.
        iv. Lessons learned.
2. **Regulatory Reporting**
    a. Submit final reports and updates to the Supervisory Authority as required.
3. **Record Retention**
    a. Retain all records of the incident and response actions for a minimum of 5 years.

Step 8: Continuous Monitoring and Improvement

1. **Audits**
    a. Conduct regular compliance audits to identify potential gaps in data security and response processes.
2. **Testing**
    a. Simulate data breach scenarios to test the effectiveness of the response process.
3. **Feedback Mechanism**
    a. Incorporate feedback from Data Subjects, employees, and regulators to improve processes.

4. Governance and Oversight

1. **Data Governance Organization (DGO)**
    a. Oversees all aspects of data protection compliance.
2. **Data Protection Officer (DPO)**
    a. Ensures the SCFHS adheres to SDAIA NDMO, PDPL, and other relevant regulations.
3. **Senior Management/Board**
    a. Reviews and approves changes to processes and policies.

5. Integration with Data Subject Rights

1. This process is integrated with the management of Data Subject rights, including:
    a. **Right to Information**

    Data Subjects must be informed of any risks to their data.

    b. **Right to Rectification**

    If data errors are found during the investigation, corrective actions must be taken.

c. Right to Compensation

Data Subjects can seek recourse for damages caused by the leak, as mandated by PDPL.

6. Tools and Technologies

1. **SIEM Systems**

   For incident detection and logging.

2. **DLP Tools**

   To prevent unauthorized data transmission.

3. **Encryption**

   To secure data during transmission and storage.

4. **Backup Solutions**

   To ensure data recovery in case of loss.