Personal Data Protection Training Program & Plan

Saudi Commission for Health Specialties (SCFHS)

Date: 01/11/2024

Personal Data Protection Training Program

1. Purpose and Objectives

The purpose of this training program is to educate SCFHS staff and stakeholders about their responsibilities under the Saudi Personal Data Protection Law (PDPL) and National Data Management Office (NDMO) frameworks. The program aims to:

a. Promote awareness of data privacy principles and best practices.
b. Ensure compliance with legal and regulatory requirements.
c. Equip participants with the tools to identify, report, and mitigate data privacy risks.
d. Foster a culture of accountability and respect for personal data protection.

2. Target Audience

The training program is designed for:

I. **Executive Leadership:** To ensure accountability and governance.
II. **Department Heads and Managers:** To oversee departmental compliance.
III. **Employees Handling Personal Data:** Including HR, IT, and licensing personnel.
IV. **Third-Party Vendors:** Providing data-related services to SCFHS.

3. Training Modules

Module 1: Introduction to Personal Data Protection

Duration: 1 hour

Content

a. Overview of the Saudi PDPL and NDMO frameworks.
b. Definitions of key terms: personal data, sensitive data, data subject.
c. Principles of data protection: purpose limitation, data minimization, accountability.
d. Penalties for non-compliance.

Learning Outcomes

a. Understand the importance of personal data protection.
b. Recognize key legal and regulatory requirements.

Module 2: Data Inventory and Classification

Duration: 1.5 hours

Content:

a. Identifying types of personal data collected by SCFHS.
b. Classifying data: general, sensitive, and critical.
c. Maintaining an up-to-date data inventory.
d. Handling sensitive data with additional safeguards.

Learning Outcomes:

a. Identify and classify personal data handled within SCFHS.
b. Implement appropriate security measures based on data classification.

Module 3: Data Processing and Consent Management

Duration: 2 hours

Content:

a. Legal basis for processing personal data.
b. Obtaining, managing, and documenting consent.
c. Rights of data subjects: access, correction, deletion.
d. Case studies on consent management.

Learning Outcomes:

a. Ensure data processing complies with PDPL.
b. Establish robust consent management practices.

Module 4: Data Security and Breach Response

Duration: 2 hours

Content:

a. Best practices for securing physical and digital data.
b. Identifying and mitigating security risks.
c. Data breach response plan and notification requirements.
d. Conducting breach simulations.

Learning Outcomes:

a. Protect personal data against unauthorized access and breaches.
b. Respond effectively to data breach incidents.

Module 5: Third-Party Management

Duration: 1 hour

Content:

a. Assessing third-party compliance with PDPL.
b. Contractual obligations and data sharing agreements.
c. Monitoring and auditing third-party vendors.

Learning Outcomes:

a. Implement robust third-party management practices.
b. Ensure vendors comply with SCFHS's data protection policies.

Module 6: Privacy Impact Assessments (PIAs)

Duration: 1.5 hours

Content:

a. Overview of Privacy Impact Assessments.
b. Steps for conducting a PIA: identification, assessment, mitigation.
c. Tools and templates for PIAs.

Learning Outcomes:

a. Conduct effective PIAs for high-risk processing activities.
b. Identify and mitigate potential privacy risks.

4. Training Methods

I. **Workshops and Seminars:** Interactive sessions led by data protection experts.
II. **E-Learning Modules:** Self-paced online courses with quizzes and practical exercises.
III. **Role-Specific Case Studies:** Tailored scenarios based on departmental roles.
IV. **Simulated Exercises:** Data breach response drills and PIA exercises.
V. **Assessment and Certification:** Post-training assessments to evaluate understanding.

5. Monitoring and Evaluation

I. **Attendance Tracking:** Maintain records of participant attendance.
II. **Knowledge Assessments:** Pre- and post-training quizzes to measure learning outcomes.
III. **Feedback Mechanisms:** Collect participant feedback for program improvement.
IV. **Regular Refreshers:** Schedule annual training refreshers to reinforce key concepts.

6. Roles and Responsibilities

I. **Data Protection Officer (DPO)**

Oversee training content and delivery.

II. **Human Resources Department**

Ensure employee participation and compliance.

III. **IT Department**

Provide technical support for e-learning modules.

IV. **Department Heads**

Encourage and monitor staff participation.

7. Training Schedule

- **Duration:** 02 Months
- **Start Date:** 01/02/25
- **Frequency:** Annual training, with quarterly refreshers for high-risk roles.

8. The SCFHS Personal Data Protection Training Program is a critical initiative to ensure compliance with PDPL and NDMO regulations. By equipping staff and stakeholders with the necessary knowledge and tools, SCFHS will strengthen its data protection practices and maintain public trust.

Prepared By:
Ascend Solutions
Approved By:
Eng. Hessah Bin Mulafikh

Personal Data Protection Training Plan

1. Objective
To implement the Personal Data Protection Training Program by providing clear steps for scheduling, resource allocation, and participant engagement, ensuring compliance with PDPL and NDMO guidelines.

2. Implementation Steps

Step 1: Preparation

- **Responsibility:** Data Protection Officer (DPO) and Training Team
- **Actions:**

    a. Finalize training materials based on the approved program.
    b. Identify and appoint trainers or external consultants with expertise in PDPL and NDMO regulations.
    c. Develop e-learning modules and ensure technical infrastructure is ready.
    d. Prepare a list of employees and third-party vendors requiring training.

Timeline: 2 weeks

Step 2: Communication

- **Responsibility:** HR Department
- **Actions:**

    a. Announce the training program and plan via email, internal portals, and notices.
    b. Provide an overview of the program\u2019s objectives and benefits.
    c. Share a schedule for training sessions, e-learning deadlines, and assessment dates.

Timeline: 1 week

Step 3: Training Delivery

- **Responsibility:** Trainers, IT Department, HR Department
- **Actions:**

    a. Conduct workshops and seminars as per the program modules.
    b. Roll out e-learning modules with progress tracking enabled.
    c. Facilitate role-specific training sessions with real-world case studies.
    d. Organize simulated exercises for breach response and Privacy Impact Assessments (PIAs).

Timeline: 1 month

Step 4: Assessments and Feedback

- **Responsibility:** DPO and Training Team
- **Actions:**

    a. Administer post-training assessments to evaluate knowledge retention.
    b. Collect feedback through surveys or interviews to identify areas for improvement.
    c. Issue certificates to participants who complete the training.

Timeline: 2 weeks

Step 5: Monitoring and Follow-Up

- **Responsibility:** HR Department and DPO
- **Actions:**

    a. Maintain attendance and assessment records for compliance audits.
    b. Schedule quarterly refreshers for high-risk roles.
    c. Monitor the application of learned practices within departments and provide additional support where needed.

Timeline: Ongoing

3. Resources Required

- **Human Resources**

    a. Data Protection Officer, Trainers, and Department Heads

- **Technical Tools**

    a. Learning Management System (LMS) for e-learning modules
    b. Simulated breach response software

- **Financial Budget**

    b. Trainer fees, software licensing, and venue costs (if in-person sessions are conducted)

4. Milestones

I. **Week 1-2:** Finalize materials and infrastructure.
II. **Week 3:** Announce and schedule sessions.
III. **Week 4-8:** Conduct training and assessments.

IV. **Post-Completion:** Gather feedback and schedule refreshers.

5. Evaluation Metrics

a. Completion rate of training modules.
b. Assessment scores and knowledge improvement.
c. Feedback satisfaction rating (target: 85% or higher).
d. Reduction in privacy incidents or non-compliance issues post-training.