Personal Data Protection Initial Assessment Report

Saudi Commission for Health Specialties (SCFHS)

Date: 01/11/2024

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

Executive Summary

This report presents the findings of an initial personal data protection assessment conducted for the Saudi Commission for Health Specialties (SCFHS) in compliance with the Saudi Personal Data Protection Law (PDPL) and guidelines set by the National Data Management Office (NDMO). The assessment evaluates the current status of SCFHS's personal data management practices, identifies gaps, and provides observations to enhance compliance and safeguard personal data.

1. Awareness of Data Privacy Management Requirements

The SCFHS has demonstrated awareness of the requirements for managing personal data privacy as per the PDPL and NDMO frameworks. This includes ensuring accountability, adopting privacy principles, and maintaining secure data handling practices.

Observations

I. Awareness sessions on data privacy principles have been conducted for key staff, though periodic refreshers are recommended.
II. A formalized Data Privacy Policy exists but requires more extensive dissemination across departments.

2. Current Practices and Gap Assessment

2.1 Identification of Types of Personal Data Collected

SCFHS collects the following types of personal data:

I. **Employee Data**

Names, contact details, identification numbers, employment records, and financial information.

II. **Healthcare Professionals Data**

Certification details, examination records, continuing education data, and licensing information.

III. **Public Users Data**

Registration information, inquiry records, and feedback data.

IV. **Sensitive Personal Data**

Health data, nationality, and religion (collected for limited purposes).

Observations

I. A data inventory is maintained, but periodic reviews to ensure accuracy and comprehensiveness are needed.
II. Sensitive data collection processes require additional safeguards to limit exposure and minimize risks.

2.2 Location and Method of Storage

I. **Physical Storage**

Paper-based records are stored in secure file rooms with access restrictions.

II. **Digital Storage**

Personal data is stored in on-premises servers and cloud-based systems managed by accredited providers.

Observations

I. On-premises servers are adequately secured, but disaster recovery protocols need enhancement.
II. Cloud storage agreements include data protection clauses; however, a review of third-party compliance with PDPL is advised.

2.3 Current Processing and Uses of Personal Data

SCFHS processes personal data for:

I. Credentialing and licensing healthcare professionals.
II. Organizing and managing examinations and continuing education programs.
III. Handling employment and payroll processes for SCFHS staff.
IV. Responding to inquiries and feedback from the public.

Observations

I. Data processing purposes are well-documented, but additional controls are required to ensure that processing is strictly limited to specified purposes.
II. Consent mechanisms exist but may need updating to align with PDPL requirements for explicit and informed consent.

2.4 Privacy Challenges to Compliance with NDMO Regulations

1. **Data Minimization**

   Current data collection practices occasionally include non-essential data, posing potential non-compliance risks.

2. **Data Subject Rights**

   Mechanisms for individuals to exercise their rights (e.g., access, correction, erasure) require further clarity and streamlining.

3. **Third-Party Sharing**

   While third-party agreements exist, ensuring consistent application of data protection obligations across all vendors remains a challenge.

4. **Data Breach Response**

   An incident response plan is in place but requires regular testing and simulation exercises to ensure readiness.

Observations

I. Privacy Impact Assessments (PIAs) should be conducted for high-risk processing activities.
II. Implementing automated tools for consent management and breach detection is recommended to enhance compliance.

3. Identified Gaps and Recommendations

Area	Identified Gaps	Recommendations
Data Inventory	Incomplete and outdated data inventory.	Conduct a comprehensive review and update of the data inventory.
Consent Mechanisms	Consent forms lack clarity and do not include granular options.	Revise consent forms to ensure compliance with PDPL and provide more granular consent options.
Vendor Management	Limited oversight of third-party compliance with data protection obligations.	Perform regular audits of third-party vendors for compliance with PDPL.
Breach Response	Existing plan lacks regular testing and comprehensive documentation.	Conduct breach simulation exercises and update the incident response plan based on lessons learned.
Data Retention Policies	No formal policy to manage data retention and secure deletion.	Develop and implement a formal data retention and disposal policy.

5. Conclusion

The SCFHS has taken significant steps toward ensuring compliance with the PDPL and NDMO frameworks. However, specific gaps and challenges remain, particularly in enhancing consent mechanisms, vendor oversight, and data retention practices. Addressing these areas will strengthen the entity's overall compliance posture and minimize privacy risks.

5. Next Steps

1. Initiate a formal Privacy Impact Assessment (PIA) for high-risk processing activities.
2. Enhance data privacy awareness programs with a focus on role-specific responsibilities.
3. Develop a roadmap to implement the recommendations outlined in this report, with assigned responsibilities and timelines.
4. Schedule a follow-up assessment within six months to measure progress.

Report Prepared By:
[Ascend Solutions]

Approved By:
Hessah Bin Mulafikh

Chief Data Officer
07/11/2024