JSANDS: Data Privacy, Confidentiality, Research and Data Sharing Policy

1. Purpose

The purpose of the Confidentiality Policy is to ensure that all staff, members and users understand the JSANDS project requirements in relation to the disclosure of personal data and confidential information. It also describes the data sharing and research related to this project.

2. Scope

This policy is applicable to the data processing of health-related JSANDS data in all healthcare facilities, either public or private hospitals. It applies to the collection, processing, analysis, exchange, transmission, and sharing of health-related data. The policy sets out the requirements for the privacy and protection of any personal data in electronic, paper, or any other form.

3. Definitions

For the purpose of this policy:

MOH: Jordan Ministry of health.
JSANDS: Jordan stillbirth and neonatal surveillance system
JSANDS system: A software developed to register all the births information in Jordan and all the stillbirths and neonatal deaths.
Project: Is the JSANDS developing and implementing project .
JSANDS team: This team includes all the members who are working on this project: researchers, project team, and MoH employees who are working in the Directorate of Non-communicable diseases. Those members have access to the project information or statistics. This team doesn't include the users who are using the system in the hospitals.
JSANDS users: Health care professionals and hospitals administrative staff who have access to the JSANDS system.
ADMIN user: This is a user who have full access to all hospital and have additional privileges that

will be mentioned later.

DATA owner: Is an individual who is accounting for a data asset. In this project the data owner is the MOH.

Data protection: Covers the generation, collection, storage, analysis, use, and sharing of personal information.

JSANDS research committee: This committee includes the director of NCDS directorate, project manager, and project coordinator**.**

4. Description of the JSANDS System Data

Data collected by the JSANDS system include socio-demographic and medical characteristics of mothers and their fetuses/infants. The system also reports information on neonatal and stillbirths' indicators and statistics, such as death rates and group specific death rates. JSANDS data and information are stored in dedicated servers in the MoH in an environment that ensure the security of the health-related data and comply with all principles of personal data protection and human right to privacy.

5. Research Policy

JSANDS is intended to encourage researchers to conduct research and to inform policy makers and health practitioners for decisions on improvement neonatal and stillbirth health care quality in Jordan. It helps them to access the data and information that they need in conducting their research and in their clinical decisions.

When faced with requests for access to JSANDS data from researchers or health practitioners, the JSANDS research committee assesses each case on its individual merits to make sure that data will be treated anonymously and respectfully. Where anonymization cannot be applied, pseudonymisation of the data should be implemented. In all cases JSANDS data used for scientific research should not be disseminated in a format that enable the data subject to be identified. This practice must be followed in relation to the collection, analysis, publication and other dissemination of any personal patient's information.

5.1 Research proposals

All potential ideas for new scientific research proposed by national researchers to use JSANDS data must be carefully read and checked by JSANDS technical committee members before any data is released. These proposals are considered in terms of their rationale, methodology, compliance with the safety and ethical standards, and impacts and implications on perinatal outcomes. Practicing doctors and other clinicians with direct and current experience in perinatology are also consulted about any clinical and legal potential risks. Data requests from commercial firms and insurance agencies that have no public sector element will be declined.

5.2 Research quality

No individual is allowed to use JSANDS data for any purpose including scientific research without prior consent. Research conducted using the data and information is complied with the ethics committee rules and regulations at JUST and the MoH.

In order to maintain compliance with our data privacy and protection policies and to reassure that patients' confidentiality is protected, the request of any JSANDS data must be evaluated in light of the: research background, research main goal and objectives, research methodology, ethical approval (where appropriate), and research outcomes and dissemination plan. The JSANDS research committee team has the right to comment on the suitability of the proposed research that do not meet required standards. The committee also has the right to comment or amend any elements of the proposed research including data collection process.

5.3 Submitting an application

Researcher who are planning to conduct research using JSANDS data or statistics should contact the project manager Professor Yousef Khader (yskhader@just.edu.jo) or the project coordinator Dr. Mohammad Alyahya (msalyahya@just.edu.jo).

Researchers are required to submit a research proposal as part of an application.

6. Information Security

Protection of JSANDS data is needed against both external and internal threats such as inappropriate access by staff. Health professionals should not leave JSNADS' computers, or files unattended in the workplace. Ideally, all records, and computers should be kept in a safe environment. Sharing JSANDS information for the purpose of healthcare is acceptable to the extent that health professionals share what is necessary and relevant for patient care on a 'need to know' basis. Clinical discussion about management of patients and healthcare should be kept confidential and out of reach from those who are not involved in healthcare. All staff who come into contact with personal health information in their work place should have enough training in confidentiality and security issues.

Health professionals should be fully aware of their ethical, legal and contractual duty of confidentiality and how to keep patient information secure within their health setting.

In death review committee meetings fully anonymized data should be used. In some cases, where the committee might need further information about specific case(s) a pseudonym code as a unique reference used so that the data will only be identifiable to those who have the code or reference. To ensure that healthcare professional have clear and enough sources of information to guide them in performing their roles effectively and appropriately while at the same time assure the conformity of human rights standards through protecting patent's information.

6. Data Sharing among JSANDS Hospitals

Where health-related data are exchanged and shared among healthcare professionals and they are not belonged to the same facility, for the purposes of providing and administering health care for a women or an infant, the data privacy and confidentiality must be maintained. The exchange and disclosure of health information and data between and among healthcare providers should be limited to the medical necessity including diagnosis, treatment, coordination or continuity of care, prevention or medico-social, and social

follow-up of the mother and/or her baby. Healthcare professionals should be able to share or access health-related data necessary to care for the patient and undertake their duties based on prior authorization. All standards will be applied to ensure the security of all data being exchanged and t maintain the balance between the protection and sharing of this data.

7. Data Governance (for the JSANDS System)

Data governance arrangements utilized in JSANDS system help us to achieve our mission of providing authoritative information and statistics about neonatal and stillbirths in Jordan while complying with our ethical, legal, and governance obligations in gathering, handling and disseminating data. Different stakeholders, especially the patients, have the right to know that JSANDS data and information will be managed professionally, with high standards of privacy and confidentiality. We rely on data governance to maintain the trust between healthcare providers, data recipients and other stakeholders such as patients, patients; relatives, researchers, health care providers, health managers, policy makers, MoH.

Our governance policy enables the release of health information for wider public benefit with the mandate of protecting human right and ensuring that data providers can be confident that the system will adhere to data sharing terms and conditions.

JSANDS Steering committee

JSANDS is governed by a steering committee established at the beginning of the project. The committee has ten members who have knowledge and experience relevant to the perinatology and who have come from different health sectors (public and private). The committee has approved the data governance policy, research policy, data privacy and data sharing policies. The steering committee facilitates liaison with the relevant professional bodies and key stakeholders interested in the system.

JSANDS Technical committee

It is an advisory body that provides oversight in making decisions on data governance policies and procedures. This committee has eleven technical, administrative and professional experts in neonatology, obstetric, and registry and surveillance systems. The committee oversees the selection and presentation of clinical data, it also provides advice and guidance about the system and release of data from a clinical perspective.

JSANDS Team

Whose one of the main functions are to release JSANDS data for research purposes and to form ethical opinion of the acceptability of any activities being carried out by the JSANDS users. The team closely supervises data collection and sharing to ensure that users are diligent in preventing breaches of information security and privacy. It also performs regular monitoring and evaluation of the progress of approved research proposals and projects, covering data processing practices including acquisition, storage, use and dissemination.

Systems and tools

The JSANDS ICT systems support secure and auditable data governance processes. In particular, access to data is restricted physically to the data center and also restricted by not allowing to access the system unless the user has the required authorization.

8. Use of Mobile Application:

Any use of mobile applications for data collection or data processing must be accompanied by security measures that provide for the authentication of the person concerned, the encryption of the transmitted JSANDS health-related data, and user or patient information standards on how the health-related data that is collected will be used.

9. Women's right to privacy during childbirth

All women personal information including previous stillbirths and/or stillbirths, previous apportions, marital status, mode of delivery and causes of deaths, especially genetic causes,

are completely protected and confidential. Data may be disseminated in aggregate fashion. This to eliminate the possibility of being identified through the system.

10. Gender as a social determinant of health

Gender is a key social determinant of health and as such interacts with culture, religion, ethnicity, education and social and economic background. JSANDS policies acknowledge and address these determinants in its actions, especially in the statistical reports.

11. Promotion and use of sex disaggregated data (SDD) and gender analysis

JSANDS policies and procedures promote the use of quantitative and qualitative data disaggregated by sex, age and other relevant social stratifications. They also strongly encourage scientific researchers and health care practitioners to analyze the complex effects of social and cultural factors on perinatal health and the reduction of gender biases in health information.

12. General rules

Any member working in this project is responsible to keep confidential any information obtained during the work on this project. The confidential information includes, but is not limited to, information relating to:

- Patients (mother or baby or husband)
- Hospital information **,** number of births deaths or any information related to the hospital.
- JSNADS System access information, username or password for the users of the system are confidential.

In order to increase the confidentiality the JSANDS system is built with many features that

help in reducing the data breaching and guarantees the confidentiality.

12. System restrictions to guarantee the confidentiality:

- It is not allowed to enter the system without username and password.
- There are three user categories:

  - **Admin** (FULL SYSTEM ADMIN): This user has full privilege on the system, can create users, reset user password, enter the new records, access the indicators for all the hospitals. During the project development and implementation, this user is given to the following members: Project director (prof. Yousef KhAder), Project manager (Dr. Mohammed Alyahya), project technical manager (Eng. Anas Matalkah).

  - **Hospital admins**: Each user of this type has privilege on a specific hospital and can access this hospital information in addition to entering the records as the normal user. The additional privileges are the following:

  -modifying records.

  -accessing the hospital statistics and indicators.

  -exporting the hospital data.

  End user: This user has privilege to enter data for a new birth and all its related information and modify the data entered by her/himself, and to change the mortality data for any birth within his/her hospital.

  For each record, the system saves who added the data (the username) and who modified it with a timestamp. This data can be accessed by the IT programmers only upon a request from the data owner.

  To guarantee data confidentiality between hospitals, in case the baby is referred to another hospital, this hospital cannot access the baby information unless they have the mother national ID.

JSANDS team

- JSANDS team includes all the members working stillbirth and neonatal mortality data at the Surveillance unit at the Directorate of Non-communicable diseases at Jordan Ministry of Health. This does not include the users in the hospital.

- The team should not share or disclose any data about the mothers or their babies to the public or anybody.

  The team is not allowed to share any information related to the collected data from the hospitals without taking the permission from data owners (MOH for the MOH hospitals and the hospital management for the other hospitals).

JSANDS users

- JSANDS users refer to staff in the hospitals who enter, check, and manage data in JSANDS system. Each hospital has two user categories: Admin user and end user.
- End users have the privilege of adding new birth, stillbirth, and neonatal death and has the privilege to modify the data when it is needed. The system will allow the end user to modify the data that he entered it previously or they can add mortality information to any birth even if it is not entered by her/him.
- Admin user has the normal user's privilege in addition to the privilege of viewing the hospital's indicators, report, and statistics.
- Any user in the hospital (admin or normal) is not allowed to share the mothers nor the babies' data with any person.
- The Admin user is not allowed to share the hospital indicators, report, and statistics with any person without taking the permission from the data owner.
- It is the responsibility of the users (admin or normal) to change their passwords frequently.
- It is not allowed to share the JSANDS system passwords with anybody.
- In each hospital there are computers provided by JSANDS project, JSANDS system is operating on those machines, the users are not allowed to use any other software on those computers therefore there are no privileges to install or modify the software on those machines.
- The JSANDS computers were given to the focal points in each hospital, and they should protect those machines from any damage and inform the JSANDS team if they notice any physical or software problem.

Contacting us

If you would like to contact us to understand more about this Policy or wish to contact us concerning any matter relating to the JSANDS Information, you may send an email to ykhader@just.edu.jo or to msalyahya@just.edu.jo .

This document was last updated on May 11, 2020