Data Management Plan for the “PureCell Project: Towards Precision Medicine” Project

1. Introduction

This Data Management Plan (DMP) outlines the procedures and policies in place for the management of biological samples and associated data at INAB.

INAB is committed to maintaining the highest standards of data security and privacy, adhering to the requirements of ISO27001 and the General Data Protection Regulation (GDPR). This document details the lifecycle of data, from acquisition to storage, access, and eventual disposal, ensuring compliance with regulatory standards and best practices.

2. Data Acquisition and Pseudo-Anonymization

Collection of Biological Samples

Biological samples are collected following standardized protocols to ensure the integrity and consistency of the data. Each sample is assigned a unique identifier to maintain traceability while protecting the identity of the individuals from whom the samples were obtained. Personal identifiable information (PII) is separated from the samples at the point of collection, ensuring that the data remains pseudo-anonymized throughout the process.

Pseudo-Anonymization Process

To enhance privacy, a rigorous pseudo-anonymization process is applied. This involves:

1. **Separation of Identifiers**: Direct identifiers such as names, social security numbers, and contact information are removed from the dataset.
2. **Assignment of Unique Codes**: Each sample is assigned a unique code that cannot be traced back to the individual without access to a separate, secure key file.
3. **Controlled Access to Key Files**: The key files that map unique codes to personal identifiers are kept at the collection site and they are not transferred to INAB.

3. Data Storage and Infrastructure

Physical Storage Environment

The physical infrastructure supporting data storage is designed to ensure maximum security and integrity. Key features include:

1. **Controlled Access**: Physical access to data storage facilities is restricted to authorized personnel through the use of access cards, biometric systems, and security personnel.
2. **Environmental Controls**: The facilities are equipped with environmental controls to protect against hazards such as fire, flood, and temperature fluctuations.
3. **Redundancy and Disaster Recovery**: Data storage systems are equipped with redundancy features to prevent data loss in the event of hardware failures. Regular backups are conducted and stored in geographically separate locations to ensure disaster recovery capabilities.

Logical Access Controls

Logical access controls are implemented to prevent unauthorized access to data. These controls include:

1. **Authentication and Authorization**: Access to data is controlled through robust authentication mechanisms, including multi-factor authentication (MFA) and role-based access control (RBAC).
2. **Encryption**: Data at rest and in transit is encrypted using industry-standard encryption protocols to prevent unauthorized access and ensure data integrity.
3. **Monitoring and Auditing**: Continuous monitoring of access logs and auditing of access records are conducted to detect and respond to any unauthorized access attempts promptly.

4. Data Access and Sharing

Access Policies

Access to pseudonymized data is granted based on the principle of least privilege, ensuring that individuals only have access to the data necessary for their role. Access policies are clearly defined and regularly reviewed to adapt to changing requirements and emerging threats.

1. **Role-Based Access Control (RBAC)**: Access is granted based on roles, with each role having predefined access rights.
2. **Access Requests and Approvals**: Access requests must be formally submitted and approved by designated authorities before access is granted.

3. **Periodic Access Reviews**: Regular reviews of access permissions are conducted to ensure compliance with access policies and to revoke access when no longer required.

Data Sharing Agreements

When data sharing with external entities is necessary, strict protocols are followed to ensure compliance with GDPR and ISO27001 standards:

1. **Data Sharing Agreements (DSAs)**: Formal DSAs are established, outlining the terms and conditions of data sharing, including data protection obligations and responsibilities.
2. **Data Minimization**: Only the minimum amount of data necessary for the intended purpose is shared.
3. **Secure Transfer Methods**: Data transfers are conducted using secure methods, such as encrypted file transfers and secure data exchange platforms.

5. Data Backup and Recovery

Backup Procedures

Regular backups are a critical component of the data management strategy, ensuring data availability and integrity in the event of data loss or corruption. The backup procedures include:

1. **Regular Backup Schedules**: Data is backed up at regular intervals, with the frequency determined by the criticality of the data.
2. **Multiple Backup Copies**: Multiple copies of backups are maintained to provide redundancy.

Recovery Procedures

In the event of data loss, the institute has robust recovery procedures to ensure data restoration with minimal disruption:

1. **Disaster Recovery Plan (DRP)**: A comprehensive DRP outlines the steps to be taken in the event of a data loss incident, including roles and responsibilities, recovery procedures, and communication protocols.
2. **Regular Testing**: The effectiveness of backup and recovery procedures is tested regularly to ensure preparedness.
3. **Incident Response Team**: A dedicated incident response team is trained to handle data loss incidents and coordinate recovery efforts.

6. Compliance with ISO27001 and GDPR

ISO27001 Compliance

INAB is committed to maintaining ISO27001 certification, demonstrating adherence to international standards for information security management. Key aspects of ISO27001 compliance include:

1. **Information Security Management System (ISMS)**: An ISMS is in place to systematically manage and protect data, incorporating policies, procedures, and controls.
2. **Risk Management**: Regular risk assessments are conducted to identify and mitigate information security risks.
3. **Continuous Improvement**: The ISMS is subject to continuous monitoring and improvement, with regular audits and reviews to ensure ongoing compliance.

GDPR Compliance

Compliance with GDPR is paramount to protect the privacy and rights of individuals whose data is processed. Key aspects of GDPR compliance include:

1. **Data Protection Impact Assessments (DPIAs)**: DPIAs are conducted for all new projects involving the processing of personal data to identify and mitigate privacy risks.
2. **Data Subject Rights**: Procedures are in place to respond to data subject rights requests, including access, rectification, erasure, and restriction of processing.
3. **Data Breach Notification**: In the event of a data breach, timely notifications are made to the relevant authorities and affected individuals, as required by GDPR.

Awareness Campaigns

Awareness campaigns are conducted to promote a culture of data protection and security within the Institute. These campaigns include:

1. **Communication Channels**: Regular communications, such as newsletters and emails, are used to share updates and reminders about data protection practices.
2. **Workshops and Seminars**: Interactive workshops and seminars are held to engage staff and provide practical guidance on data protection topics.
3. **Incident Drills**: Simulated data breach scenarios are conducted to test and improve the institute's response capabilities.

7. Conclusion

INAB is dedicated to maintaining the highest standards of data protection and security in the management of biological samples and associated data. By adhering to the requirements of ISO27001 and GDPR, the Institute ensures the privacy and integrity of data throughout its lifecycle. This Data Management Plan provides a comprehensive framework for the secure handling, storage, and sharing of data, supporting the institute's mission to conduct research and provide services in a responsible and ethical manner.