PUBLIC HEALTH FOUNDATION OF INDIA

Central Research Data Repository (CRDR)
Clinion – Data Security

21/02/2019

Prepared By:	Archana Bhattacharya	Senior Manager, CRDR	Archana 21/Feb/2019
Reviewed By:	Abhishek Srivastava	IT Head Shrivast	
Reviewed By:	Geetha Nambiar	Grants Admin Head	Geetha 21/2/19.
Reviewed By:	Dr.Dimple Kondal	Sr. Scientist, Biostatistician	Dimple 22/2/19
Reviewed By:	Narayan Chatterjee	Special Advisor-Government & NGO Relations	19 Mar 19
Approved By:	Dr. D. Prabhakaran	V.P. Research and Policy	

CRDR – Data Security
PHFI/IIPH

Dated:21/02/2019

TABLE OF CONTENT

19 Mar 19

Summary

Central Research Data Repository (CRDR)

This document encompasses the ways in which data derived from research, operational and implementation programmes (data) once accrued at the Public Health Foundation of India (PHFI) and its constituent Indian Institutes of Public Health (IIPHs), may be stored, archived and shared in the secured environment of Central Research Data Repository (CRDR) platform.

This policy is specific to PHFI and is meant to safeguard the investigators and team members involved in the collection of data and the organization. At PHFI, the Research Management Committee (RMC), Internal Technical Review Panel, Central Research Data Repository team, Principal Investigators and the relevant project team staff are entrusted with managing and protecting the data arising from various projects undertaken. This policy applies to all projects that are undertaken at and by PHFI which is archived or managed through the CRDR platform.

This will complement the institutional policies and guidelines on intellectual property rights, ethics review and financial management at PHFI/IIPHs and will not supersede them. Guidelines or policies that are drafted to manage authorship criteria will be independent of this document.

I. **Definition: Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.**

II. This policy is applicable to all PHFI/IIPH staff, researcher, faculty, students and consultants who are involved in projects/programmes undertaken by and at PHFI/IIPHs and aligned to as per the requirement of funding agencies.

III. The policy will be applicable for all the projects by the date of approval of this policy. For new studies as per the requirements specified by the donor, all the documentation will be carried out in repository.

IV. The PI will have exclusive access to the data generated by the respective project and to others that are granted permission by the PI. Team members will have a right to review that portion of the data that was generated/created by them. PHFI will have access to the data as necessary for compliance and other purposes. In case the sponsoring agency/collaborators wishes to access data generated by the respective project, this will be based on the terms and conditions and policies (MOUs/agreements between PHFI and the donor and collaborators, data sharing policy, PHFI corporate policy and conflicts of interest policy) defined and followed by the PI and the collaborator/sponsoring agency.

V. Data will be maintained by PHFI for at least **seven years** after completion of the project or as specified by the funding agency. Appropriate scanned copy of paper and electronic storage mechanisms would

19 Mar 19

be made so that data can be accessed as required. Data will not be destroyed or removed without prior approval of the Research Management Committee.

VI. Transfer of data from PHFI to another organization after the seven years period if required; must be approved by RMC. PHFI would retain copies in all such cases.

Public Health Foundation of India * New Delhi

19 Mar 19

CRDR – Data Security

PHFI/IIPH

Dated:21/02/2019

1. INTRODUCTION

Clinical Research Data Repository (CRDR): A Central database repository is a logical and physical grouping of data from related but separate databases. This is usually done when there is a 'higher purpose' for the data, but the data items needed to do this reside on different databases. In these cases a repository is necessary to bring together the discrete data items and operate on them as one. The application is 21 CFR part 11 complaint and is complying with all applicable security norms.

Ways of securing the data includes:

- Data Encryption - converting the data into a code that cannot be easily read without a key that unlocks it.
- Data Masking – masking certain areas of data so that a personnel without the required authorization cannot view it.
- Data Erasure – ensuring that no longer used data is completely removed and cannot be recovered by unauthorized people.
- Data Backup – creating copies of data so that it can be recovered if the original copy is lost.

The PHFI has developed the policy on data security to safeguard final research data stored in the CRDR platform. The Central Research Data Repository will be based out in Plot No. 47, Sector 44, Institutional Area, Gurgaon - 122002, Haryana.

1.1 DEFINITION

Terms	Meanings
Funder	The name of the funding agency who supports/funds the institution to carry out the research work.
Data Security	Data Security concerns the protection of data from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls, and other safeguards to limit accessibility.
Data sharing rights	Rights and responsibilities of various actors involved in data sharing including funders
Data Management Plan Requirements	Requirements to provide information on data management and/or sharing activities as part of the project plan
Retention Requirements	An indicator of the minimum time period that data assets should be retained and the institutional agent that should be responsible

Public Health Foundation of India
New Delhi

19 Mar 19

Terms	Meanings
Documentation Requirements	Documentation suggested by PHFI management or funders that should be provided to help researchers to access and use research data produced.
Central Database Repository	A Central database repository is a logical and physical grouping of data from related but separate databases with built in-depth access control rules.
PHFI/IIPH	Public Health Foundation of India/Indian Institute of Public Health

2. APPLICATION SECURITY

2.1 PASSWORD POLICIES

User is enforced to change the password at the time of initial login.

- Setting a strong password is enforced to the user by having the minimum and maximum password length and by allowing special characters in the password.
- If the user tries to login with a wrong password continuously for three times, the user will be locked out. Tt can then be unlocked only by the administrator. A mail will be sent to the user which contains the new password.
- The system enforces the user to change the password after certain period. Password history is maintained in the database which does not allow the user to enter the current password at the time of changing the password.

2.2 ENCRYPTION MECHANISM

Secure Socket Layer (SSL) standards are followed for data transfer through a secured network. Confidential user information is protected by using this protocol. SSL uses encryption algorithm which compress the data and signs it with a private key before the data transfer occurs. By performing client server authentications, SSL uses message authentication codes to ensure data integrity.

- All the passwords are encrypted and saved in the database.
- The data provided in the application pass between the web server and the web browser in encrypted format.
- The application is secured with https in the URL.

Public Health Foundation of India * New Delhi

19 Mar 19

- URL tampering is not allowed in the application.
- The user is logged out if he/she tries to tamper the URL.

3. *DATA SECURITY*

3.1 *DATA STORAGE*

- Access to the application is limited to the authorized individuals.
- Data is stored in the database only when entered by authorized individual by providing the necessary authentication.
- Transaction management is used when electronic case report forms (CRFs) are committed to database to ensure data integrity for the database.
- Audit log is maintained for any change made in the uploaded data.
- Data change in the CRFs must be authenticated by providing the password.
- Activity log is maintained for all the activities performed on the application.

3.2 *DATA SHARING*

No caching implemented in the system which doesn't allow the user to save the login details. Back and forth buttons access is not allowed. The user is navigated to the home page if he/she tries to navigate by using the back and forth buttons. The database can be accessed only through the application which is password protected. Right click disabled in the application by which a user cannot copy the content of the page. The user is logged out if no user action takes place for a certain amount of time. Regular backups are taken to ensure the data back-up for recovery. Daily incremental back-up and Weekly 3 full back-up are carried out and maintained in a secured server. Security firewalls are installed to prevent the unauthorized access to the system. The authorization of data access is given by the administrator. The administrator can restrict/allow the user to access the data.

3.3 *URL CANNOT BE ACCESSED FROM EXTERNAL IPs UNLESS THE PERMISSIONS HAVEBEEN ALLOTTED.*

- System admin can either permit the access to requested IP or deny the permissions.

3.4 *GENERAL SECURITY*

Public Health Foundation of India
New Delhi

19 Mar 19

CRDR – Data Security

PHFI/IIPH

Dated:21/02/2019

- CRDR Servers are hosted in the secure PHFI premises and have redundancy with Virtualization in place.

- Hosted network is protected behind firewalls and protected by gateway antivirus and is regularly monitored .

- Server data is backed up regularly, as per back up and restoration policy

- Physical and environmental security – access to restricted areas like data center is only for authorized personnel. Surveillance systems and monitoring Sensors are also in place.

- Data in servers are secured and same is only accessible through VPN and given access to only authorized user(s).

- Data in transit is encrypted through SSL.

- Remote working is done only through secured mechanisms like VPN.

Public Health Foundation of India
New Delhi

19 Mar 19