NATIONAL FAMILIAL HYPERCHOLESTEROLAEMIA REGISTRY

Data Management Plan

Version 1.0

Endorsed 15 October 2018

Australian Atherosclerosis Society - Secretariat: Your Secretariat

PO Box 5436 Chittaway Bay, NSW 2261 Australia

Telephone (+612) 4356 0007 Facsimile (+612) 4355 4347
E-mail admin@yoursecretariat.com.au

AAS ABN 17929443544

CONTENTS

- **Data security** 3

Physical sercurity 3

Network security 3

System security 3

Other technological security measures 4

- **Policies and procedures** 5
- **Contractual and licencing arrangements, and confidentiality agreements** 5
- **Training** 5
- **Data storage** 5
- **Purpose of data storage and usage** 6
- **Data Access Conditions** 6
- **Communications** 6

This data management plan has been developed in consultation with the Centre for Comparative Genomics (CCG), Murdoch University. The National Familial Hypercholesterolaemia (FH) Registry was created using the Rare Disease Registry Framework, which was developed by the CCG.

➢ Data security

Physical security

The FH registry is currently hosted on-premises at Murdoch University, in a data centre. Access to the data centre is controlled via key access, and access to the building housing the data centre is mediated via smart-card access (outside of office hours.)

The future hosting environment is proposed to make use of servers and other services provided by Amazon. Amazon provide details of their physical security arrangements here: https://aws.amazon.com/compliance/data-center/controls/

In both the current and future hosting scenarios, in the event of a compromise of physical security, all registry data (including the clinical and demographic information databases) are stored encrypted-at-rest. This means that the registry data will be totally unreadable if the disk infrastructure were accessed offline, for example after being removed due to theft.

(see https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html for the AWS database encryption details)

Network security

The FH registry is hosted on a server environment located at the CCG, at Murdoch University. Key components of the system (clinical information database, demographic information database, application server, web server) are located within an isolated environment dedicated to registry hosting. This means that the FH Registry is not accessible by non-registry admins (ie. CCG developers) and that the computer running the software is not running other non-registry systems for other purposes in parallel.

Associated network infrastructure is protected by a Firewall (pfSense), that restricts access to the system. Additional security is provided by an Intrusion Detection System (IDS; Snort) that scans incoming network requests for potential attacks and attempted security breaches. Network hosts known to have been behaving maliciously are pre-emptively blocked via a distributed block-list to which the IDS is subscribed.

System security

All access to the FH Registry application is via authenticated accounts. Appropriate permissions, defining role-based access, are set by the Registry Coordinator or other authorized staff. Two-factor authentication can be required for access to the system, and this is recommended for administrator and clinician accounts.

Web access to the system is limited to secure, 'HTTPS' access, with all data encrypted in transit. Transport Layer Certificate security is used to secure the domain so that data cannot be intercepted or spoofed.

Administrative access to the system is limited to CCG staff only, with access only via the 'Secure Shell' system.

Other technological security measures

The FH Registry enforces a number of rules relating to user log-in and access:

1. Mandated password length and complexity
2. Maximum number of failed logins (all logins, successful or denied, are logged, including IP address and other identifying data)
3. User accounts are deactivated once the number of permitted login attempts has been exhausted
4. Passwords for user accounts expire after a defined time (e.g. 3 months)

Additionally, site-wide security can be increased by:

1. Restricting access to IP addresses within particularly countries (e.g. Australia)
2. Blocking or permitting particular IP addresses (e.g. in the event of a detected attack)

Within the application, measures are taken to ensure that a given user is only able to access the data permitted by their role within the system:

1. Access rules defined by user role – for example, form data can be restricted so that it can only be seen by particular users
2. Access rules defined by working group – effectively, partitioning of the registry data. Users belonging to a particular working group are denied access to view or edit data belonging to any other working group.

To allow for auditing of the system, the application maintains an audit trail of changes to all data records over time. This includes a log of all of the following options, within both the demographic and clinical information databases:

1. Creation of tracked database objects
2. Deletion of tracked database objects
3. Update/Edit of tracked database objects

Each audit log entry includes:

1. The user making the change
2. The time at which the event occurred
3. The details of the change, including a full representation of the data before and after the change (in the case of a Creation or Update event)

Additionally, a longitudinal view of changes to relevant data fields is available within the application.

Overall data security obligations and requirements are also set out in the Software Hosting and Services Agreement.

➢ Policies and procedures

Murdoch University staff are bound by all relevant policies and procedures, including:

- Murdoch University IT Conditions of Use Policy
- Murdoch University Information Security Incident Management Policy
- Murdoch University ICT Security Policy

Overall data security obligations and requirements are set out in the System Hosting agreement. This includes the protocol to be followed should a data breach incident occur.

The CCG tracks application releases, including associated database migrations, in an issue management system. Any issues that occur are recorded.

➢ Contractual and licencing arrangements, and confidentiality agreements

Confidentiality and licensing arrangements are set out in the Software Hosting and Services Agreement.

➢ Training

The FH Registry includes system and user documentation, which is available online at:
https://muccg.github.io/rdrf/docs/

The CCG provides one-on-one user training to the Registry Coordinator.

A user manual for the FH Registry can be accessed through the landing page of the FH Registry:
https://fhregistry-international.com/

➢ Data storage

FH Registry data is stored in two PostgreSQL relational databases – one database for demographic (e.g. identified) data, and a second database for clinical data.

Data is stored on disk infrastructure that is encrypted-at-rest.

Data is backed up off-site, daily, in encrypted form (a long, secure password is required to decrypt the backup archive).

The database schema is defined by the FH Registry application. Additional, FH Registry specific, schema information is defined by the 'YAML' configuration for the registry that is stored in a private, secure repository. Changes to the global RDRF schema, as well as the FH-specific schema, are versioned, so that schema changes and any associated data migrations can be tracked over time.

➢ Purpose of data storage and usage

Purpose of data storage and data usage are outlined in the Patient Information Sheet. This can be access through the landing page of the FH Registry:
https://fhregistry-international.com/

➢ Data access conditions

Data access conditions are outlined in the Charter, Protocol and Guidelines document. This document can be access through the landing page of the FH Registry:
https://fhregistry-international.com/

➢ Communications

Details of the Registry framework, hosting arrangements and data confidentiality will be communicated to potential participants via the Patient Information Sheet.