REB Questions regarding Health Research BC REDCap

The following are often asked data management and REDCap questions by ethics committees. This is not a comprehensive list, and the answers to these questions can differ from project to project.

Question 1 (RISe #8.4B): Will personal health information or personal identifiers be collected?

Answer: The answer is project-specific. As it pertains to the use of Health Research BC REDCap, our policy stipulates the following:

Direct patient identifiers such as full name, address, SIN, MRN, CareCard, patient number, etc. are not to be stored in the Health Research BC REDCap platform – except for identifiers approved by the corresponding REB

Subject ID codes should be used to ensure privacy and confidentiality.

Subject ID codes based on date of birth, ethnicity, MRN, hospital record number, and residency should be avoided. Variables that can identify the person either alone or in combination similarly must be avoided. Instead, subjects should be coded with a study number that is not identifying of the individual. If needed, the hospital's unique record number can be linked to the study subject's number in a separate password-protected and encrypted document. This further decreases the risk of personal information becoming accessible should the information be lost or stolen.

Relevant Documents:

- Health Research BC REDCap Privacy and Security Agreement

Question 2 (RISe #8.5A): Who will have access to the data at each stage of processing and analysis, and will a current list of study personnel names (including co-investigators) be maintained in the study file?

Answer: REDCap has an authorization matrix, allowing different members of the study team to have different levels of access (none, read-only, or edit) to data entry forms, and access to project management and data export tools. REDCap enforces the authorization granted to each user by providing and/or enabling certain functions, tabs, links and buttons according to granted privileges. REDCap includes a full audit trail which records all operations on the data, including viewing and

exporting. The audit log records the operation, date and time, and the user performing the operation, permitting review of the audit trail as necessary.

At Health Research BC, only the Health Research BC DM Team staff are Super Administrators. The Super Admin is the role within the system that creates user accounts at the request of the Principal Investigator (PI) or the Project Administrator (PA). All accounts created require the first and last name of the user, and their approved institutional email address. New users are emailed a password link, where the user can set their password and a security question. Only the account holder knows their password and user accounts can be reused for other studies as directed by the PI or PA. User accounts also follow PopData security policies, which among other safeguards, include two-step authentication.

Both the Super Admin and designated users (QI or PA) can grant permitted users access to a specific study. Access to specific features can be turned on or off depending on the user's role such as Administrator, Manager, Data Entry, Designer, and monitor of data. For each instrument "none", "read-only" and "edit" can be assigned as well as data extraction rights can be granted for an entire study.

Note: PI should be aware that REDCap has self administered training modules. However electronic training logs are not kept for this self-guided user account activity and it is recommended that the QI tracks and logs all training in order to satisfy ICH Good Clinical Practice (GCP) requirements.

Relevant Documents:

- SOP 101 – Health Research BC REDCap Adding New Users
- SOP 102 – Health Research BC REDCap User Training
- Creating new PopData accounts: https://my.popdata.bc.ca/account/register/

Question 3 (RISe #8.5.B): Describe how the data will be stored (e.g. computerized files, hard copy, video recording, audio recording, PDA, and other).

Answer: REDCap has the capacity to store 'live' data for multiple, ongoing study databases simultaneously where each individual study database has the option of supporting multiple centers. The actual data for each database is stored on a private, relational MySQL database at the data centre which is located on-site at PopData, BC.

All information and Data are backed-up on secure servers and encrypted media, protected by locks and alarms within a high security zone. Encrypted backup media are also stored in a secure off-site location, as per internal policies and procedures.

Relevant Documents:

- https://www.popdata.bc.ca/index.php/privacy/policies

Question 4 (RISe #8.5C): Describe the safeguards in place to protect the confidentiality and security of the data.

Answer: Population Data BC will utilize stringent physical safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification of data.

Population Data BC will utilize stringent technological safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification of data.

Population Data BC will utilize stringent organizational safeguards to protect against loss, theft, unauthorized access, disclosure, copying, use or modification of data.

Population Data BC enforces stringent safeguards for the transfer of data, from both data stewards into Population Data BC's secured facilities, and from Population Data BC to researchers for approved research projects.

Relevant Documents:

- https://www.popdata.bc.ca/index.php/privacy/policies

Question 5 (RISe #8.6A): Describe what will happen to the data at the end of the study including how long the study data will be retained and when and how the data will be destroyed.

Answer: The answer is project specific and the responsibility of the PI. As it pertains to the data stored in Health Research BC REDCap, upon request from the PI, the study can be archived. All study data and logs remain stored in REDCap, where it can be accessed and unarchived upon request if necessary. Study data remains on the servers unless otherwise specified by the study team. Any data destruction is carried out according to a study team's plan.

Relevant Documents:

- https://www.popdata.bc.ca/researchers/resources/REDCap

Question 6: When surveys are completed anonymously online through advertisement and there is no verification/informed consent conducted with research staff, how do investigators know that respondents are real subjects and not trolls or bots? How does one validate their survey findings?

Answer: Teams can turn on Google reCAPTCHA, which helps with spam generated by 'bots'.
The Google reCAPTCHA feature can be enabled to help protect your public surveys from abuse from 'bots', which are automated software programs that might enter trash data into your survey. A 'captcha' is a Turing test to tell humans and bots apart. It is easy for humans to solve, but hard for bots and other malicious software to figure out. By enabling Google reCAPTCHA on your public survey, you can block automated software while helping welcome your survey participants to begin your survey with ease.

As for trolls (people entering false data into a questionnaire), teams should ensure that they include extremely specific questions that only their study population would be able to answer, such as open-ended questions that require details, etc.

For validation, teams should have clear exclusion criteria to be used during data clean up, where respondents/answers with inadequate information would be excluded/filtered from data analysis, much the same as they would for any other type of study.

Additional Resources:

Research Ethics Approval information - http://www.phsa.ca/researcher/ethics-approvals/research-ethics-approval