CHICKEN SOUP FOR THE BUSY COORDINATOR

DEC 2018

HOW SHOULD RESEARCH DATA BE MANAGED & STORED?

Dr. Tan, a medical officer had created a database to collect information for his research on 100 patients with Type 1 diabetes for his department and saved the database in a thumb drive. He recently thought he had misplaced the thumb drive and was frantically looking for it. Fortunately, the patient service associate kept the thumb drive and returned it to him.

What if the Dr Tan's thumb drive was indeed missing/lost?

If the thumb drive containing subject identifiers was missing, it would be considered as a serious breach of confidentiality according the Human Biomedical Research Act (HBRA), Personal Data Protection Act (PDPA), institutional policies and all other relevant regulations. Dr Tan would be required to notify the data breach (loss of the thumb drive) immediately to the NHG DSRB within 24 hours from the time that he was aware of the breach.

How should the research data be stored? What is a standing database?

When the research had completed, Dr Tan should consider storing the information as a standing database with the NHG DSRB. Standing databases are often created and maintained for purposes that are unrelated to research. However, if a database is created with the intention of using the stored data for future research, the creation of such a database will require the NHG DSRB's review and approval. Individual research projects extracting data from such databases will also require the DSRB review and approval. For more information on standing database, refer to NHG Good Practice Guidelines for Standing Databases & Tissue Banks.

Dr Tan is strongly encouraged to use the Research Electronic Data Capture (REDCap) to capture his data. If the REDCap cannot fulfil his data requirements, alternative data capturing tool or equipment could be explored. However, Dr Tan must ensure that these alternatives must comply with his institution's IT security recommendations.

How should data be managed?

Dr Tan should ensure that:

- The study responsibility log clearly states who in the research team is responsible for data management activities such as transcription of data to CRFs, data entry and analysis (where applicable).
- Electronic databases should be stored in a secure computer, preferably stored on a stand-alone computers, password protected and with limited access, rather than on a common drive
- The research data recorded, handled and stored in a way that allows its accurate reporting, interpretation and verification.
- The databases should not contain subject identifiers and the data linking subjects' identifiers and the subjects' identification codes should be stored separately. The master list linking participants names to the study ID code should be maintained by the PI and kept in a secure location (i.e. limited access).
- Subjects' identifiers (data) should not be stored in a portable devices (e.g. thumb drive, personal hard disks).
- Databases must be stored in a de-identified/ coded format. The code must be a random linking code. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual.

References:

1. *NHG Addendum to the Investigator's Manual Dec 2018*
2. *NHG Proper Conduct of Research SOP 501-B08: Data Collection and Handling, 501-A02: Responsibilities of the Research Team*
3. *NHG Online NHG Standing Database/ Tissue Bank Application Guidebook Version 1*

Additional Readings:

1. *NHG Research Data Policy*
2. *NHG Data Sharing Policy*
3. *NHG Personal Data Protection Policy Guide Rev 5 – Section 11*
4. *Personal Data Protection Commission Singapore. Main Advisory Guidelines: Advisory Guidelines on Key Concepts in the Personal Data Protection Act, The Protection Obligation (Chapter 17)*
5. *Human Biomedical Research Act 2015*

Article Contributed By: **Ms. Xu Xiaoying, Manager, Tan Tock Seng Hospital**
Edited By: NHG-RDO

Proudly brought to you by: Clinical Research Coordinator Society (CRCS)
(researchcoord@nhg.com.sg)