Research Ethics Board
(613) 562-6262 ext. 4003
REB@bruyere.org
Bruyère Research Ethics Board

BRUYERE REB GUIDELINE

DATA MANAGEMENT PLANNING: COLLECTION, STORAGE, TRANSFER, AND DESTRUCTION OF RESEARCH INFORMATION

Purpose

This guideline applies to data collected, used, stored, transferred and destroyed as part of any research project carried out at Bruyère Continuing Care, and the Bruyère Research Institute.

This document is intended to assist researchers in better understanding the legislative standards and policies in place to protect personal health information during the process of collection, use and storage of research data, to address the secure transferring of the data from the source site, and to ensure the appropriate disposal of confidential materials.

Under provincial health privacy legislation, health information custodians (i.e., a hospital) have a responsibility to protect personal health information from theft, loss, unauthorized use, disclosure, copying, modification, or disposal. There is a positive obligation for custodians to notify individuals of any breach of their privacy.

Coded Data: This refers to data that is collected, shared and stored under an alpha-numerical code that excludes the research participant's name, birth date, or any other identifying information.

1. When do I code the data containing personal health information?

a) For privacy protection, all research-related personal health information must be coded, except in extraordinary circumstances as approved by the research ethics board, at the earliest opportunity during the collection of data to prevent the identity of an individual from being linked directly to the data being collected. The coded data and the master code list must be stored separately, in a secure manner.

b) The subject's initials or any other personal identifier may not be used as part of the code unless they are adequately scrambled and embedded with at least one other

unrelated letter. The plan for coding should be described in Section 19d) of the BREB Application, describing in detail how and when the data will be encoded to remove all personal identifiers.

c) In general, with the exception of the code assigned to the research subject, direct and indirect personal identifiers should not be included on the research data set or the data collection tool. The master code list or code key, which includes the code linking personal identifiers and data for an individual, should be stored separately from the coded personal data set or data collection tool, and stored as an encrypted, password-protected document.

2. How do I ensure proper storage of personal health information?

a) As per Bruyère Continuing Care policy (DOC 02) Storage, Retention, Destruction of Health Records, all personal health information in paper format (including health records, working notes) must be stored in a secure or locked area, either within the Health Records Department, in a health records storage room, on the unit, or in the clinic or department where the patient is being or has been followed, accessible only to authorized staff.

b) All personal health information in electronic format (including electronic patient records) is stored on the Bruyère S Drive, is password protected, and only available to authorized staff. Removable media (e.g., CDs, USB Memory Sticks, etc.) used to store confidential information must be obtained from Information Systems, who will provide encrypted USB keys for this purpose. Please note that encrypted USB keys are only a temporary storage solution.

c) All personal health information in electronic format must be stored with password protection, using a "strong" password. Please see the Bruyère Continuing Care Information Systems website on InfoNet for more information about choosing a strong password. There are additional suggestions to choosing passwords to ensure they are secure.

d) When accessing personal health information remotely through VPN (Virtual Private Networks), researchers must ensure that the information is not exposed to unauthorized users. Personal health information, as well as any confidential information must not be stored on any personal computing devices (e.g., smart phones, USB memory sticks or hard drives, tablets, laptops or home computers), only on Bruyère approved encrypted devices.

e) Never store codified (de-identified) or anonymized data in the same place as the master

code list or other identifying information.

f) In addition to the general Tri-Council Policy Statement 2, the Canadian Institutes of Health Research (CIHR) produced Best Practices for Protecting Privacy in Health Research which outlines the following principles and requirements for storing data that contain personal and personal health information. See: http://www.cihr-irsc.gc.ca/e/29072.html

1. Data should be assessed using a threat-risk vulnerability assessment, which includes seven steps (i.e., determine what assets need to be protected, determine what to protect against, assess probability of threat occurring, assess magnitude of the impact if threat occurs, assess existing safeguards, recommend appropriate additional safeguards, & update regularly).

2. To safeguard the data, organizational, technological, and physical measures should be taken.

3. Organizational safeguards include a commitment to privacy and continued emphasis of its importance by all involved in the research, a pledge of confidentiality by all involved, strict limitation of access to personal information, data sharing agreements in place between researcher/institution where applicable, clearly stipulated consequences for breaches of confidentiality, and adequate resources dedicated to privacy and security policies and procedures.

4. Technological measures include encryption, removing direct identifiers where possible, camouflaging sampling when appropriate to prevent access to private information prior to consent being given, authentication measures (e.g., passwords), special protection for remote access, virus checking programs, regular back-ups of the data, and where possible, an audit trail monitoring system to document the person, time, and nature of data access.

5. Physical measures include storing computers and files in locked rooms, storing paper files in locked cabinets, minimizing the locations where personal information is stored, precluding public access to where data is stored, routine surveillance and protection from hazards, such as fire and floods.

6. All personal health information in paper format or on removable storage media (CDs, etc.) must be stored in a locked cabinet, accessible only to members of the research team for the particular project who have submitted a Pledge of Confidentiality to the REB.

7. In Section 19 of the BREB application, indicate where the code-list will be stored and when it will be destroyed. Also describe the provisions that have been made to guarantee the secure storage of the code-list in the event that the Site Principal Investigator, or other research staff with authorized access to the code-list, no longer have a position at the research site.

8. The original master code list may be stored in the Health Records Department for safe-keeping for an approved time period. The code list is to be accompanied by an information sheet giving the project title, names of the principal investigator, a pledge stating that all copies of the code list have been destroyed (or the planned date of destruction).

9. If the principal investigator leaves the organization during the course of the study, or before the destruction date of the research data (e.g., master code list and all other data) as indicated on the original request form, **the new principal investigator must notify the Privacy Office.** REB approval of changes does not ensure continued access to Health Records.

10. Please refer to the Privacy Office for instructions on the destruction of identifiable research data.

11. The Privacy Office maintains a permanent record of all approved access to health records requests, their proposed date of destruction, and confirmation of when master code lists and all other identifiable data have been destroyed (for privacy auditing purposes). The Privacy Office tracks that the data has been destroyed, and follows up, as necessary, with the investigator if the form attesting to the destruction of the data was not completed by the identified date.

3. Length of retention

a) CIHR states that personal data should be retained as long as is necessary to fulfill the research purposes. Personal data may then be destroyed as set out in the terms of the original collection, data-sharing agreement, institutional policies and legal requirements. The Bruyère REB does not require that research data be destroyed so long as it is de-identified and properly stored.

b) In the BREB application, researchers should be explicit about what they plan to do with the data they collect, including storage, management and destruction procedures. Refer to

Bruyère-related policies (below) for more information.

c) Bruyère policy DOC 02 Storage, Retention, Destruction of Health Records reads:

"2.2 **Retention and archives:** All **paper health records** (including original legal documents such as living wills and capacity assessments) are retained for a period of 12 years (or longer, as required [e.g., 25 years if involved in clinical trials]) from:

- the last date of discharge from the clinic or program;
- their last visit as an outpatient;
- their last discharge date from **any** Bruyère program or service."

4. Transfer of identifiable and de-identifed data from the source site

a) Avoid, where possible, taking data offsite, whether in hard copy or in electronic format. Hard copies of PHI with patient identifiers may not be removed from the hospital premises unless de-identified.

b) **Section 19g) of the BREB application guidelines, requires that data containing personal identifiers should <u>not generally</u> leave the premises of the research site facility.** If data containing personal identifiers will be transferred to another facility, you will need to justify why in this section. In addition, you will need to describe the plans for the secure handling and transfer of the data including the methods to be employed to maintain confidentiality at the receiving facility. Also, you will need to include documentation demonstrating that an officer (e.g. Chief Executive Officer, Chief Financial Officer) of the receiving facility with signing authority to bind his/her corporation has agreed to store and to destroy data containing personal identifiers according to the study's protocol described in this application. This documentation would typically take the form of a Data Transfer Agreement.

c) When transporting personal health information in paper format or on removable storage media (CDs, USB memory sticks, etc.), it must either be stored in a locked container or a password protected encrypted USB (approved by Bruyère), accessible only to members of the research team for the particular project who have submitted a Pledge of Confidentiality to the REB. Some general guidelines include the following:

d) Make every effort to never leave data unattended or in non-secure locations (e.g., a locked car) as this increases the risk of accidental confidentiality breaches;

1. Ensure computers and files are password protected;

2. Consider storing data temporarily on an approved, encrypted USB memory stick;

3. Never transport ID lists, or any other data or information that affords the possibility of identifying individuals from the anonymized dataset, together with the anonymized data.

4. Always bring data collected offsite to the approved secure location as soon as possible. Always ensure that data collected off-site is de-identified as soon as possible.

5. Always exercise extreme caution when using e-mail systems to transfer data. E-mail is not secure. Safe e-mailing procedures are especially important. **Only e-mailing a password protected file between Bruyère emails is acceptable.** Refer to policy ADMIN 29 Email for details on how to properly send confidential patient information via email. Item 3.5.2 reads: The sensitive or personal health information is in an encrypted or password-protected attachment, preferably in a PDF format, and the password communicated by phone or in person (contact Helpdesk for assistance).

6. If your study is geographically broad, and data transfer via Bruyère email is not possible, you will need to use an approved, encrypted file transfer/data sharing program/platform (for de-identified or anonymized data only). Please contact the Bruyère IT department, the REB office, or your operations manager for an approved file transfer/data sharing platform.

5. Destruction/disposal of personal health information

a) Policy ADMIN 07 Destruction of Confidential Material, item 2.1 reads:

- "Dispose of all confidential documents on paper in the locked consoles identified for this purpose located throughout each site (stapled documents and those with coil bindings can be disposed of as is in these consoles). A services arrangement has been made with an external provider to empty these consoles monthly and shred the contents. In order to protect the confidentiality of personal health information, confidential information in paper form that is no longer required must be shredded before being recycled (as stated in Policy ADMIN 07 Destruction of Confidential Material, item 2.1)

b) For shredding, a commercial document shredding company provides such a service (as stated in Policy ADMIN 07 Destruction of Confidential Material, item 2.1)

c) When computers that contain personal health information are no longer needed, the IT department must be contacted for the removal of the computer. Refer to policy ADMIN 07, item 2.3: Contact Helpdesk (Information Systems department) for assistance with the destruction and recycling of electronic material in other formats, including memory sticks, hard drives, and computers. Helpdesk makes arrangements for all hard drives to be removed and physically destroyed in-house when a computer is retired.