Bruyère Continuing Care
Research Ethics Board

Risk Management Planning: Storage, transfer, and destruction/disposal of information.

A guide for investigators

This document is intended to assist researchers in better understanding the legislative standards and policies in place to protect (health) information during the process of storage of data, transferring the data from the source site, and during the disposal process.

Health information custodians (usually, 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.

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

Statutes governing use of personal (health) information state that for privacy protection, all personal Health inform**a**tion must be coded 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.

Please note that the subject's initials or any other personal identifier cannot be used as part of the code unless they are adequately scrambled and embedded with at least one other unrelated letter. **In Section 19c) of the COREB application, you will need to describe in detail how and when the data will be encoded to remove all personal identifiers.**

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.

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

Bruyère Continuing Care policy (DOC 02) states that all personal health information in paper format (including health records, working notes by health professionals, etc.) must be stored in a secure or locked area, either within the Health Information and Client Services Department (formerly known as 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.
All personal health information in electronic format (including electronic health records) is stored where physical and technical safeguards have been implemented. Removable storage media (CDs, etc.) containing PHI must be stored in secure or locked areas.

All personal health information in electronic format must be stored with password protection. It is suggested that users always choose a "strong" password. Please see the Bruyère Continuing Care Information Systems website on InfoNet for more information about choosing a good password. There are additional suggestions to choosing passwords, to ensure they are secure.

When accessing personal health information remotely through VPN (Virtual Private Networks), researchers must ensure that the information is not exposed to unauthorized users.

Never store anonymized (de-identified) data in the same place as ID lists or other identifying information.

In addition to the general Tri-Council policy statement, the Canadian Institute of Health Research (CIHR) produced a document on best practices for protecting privacy in health research. It outlines the following points for storing data that contain personal information (Canadian Institutes of Health Research, 2005).

- 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).

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

    - 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 commit adequate resources to privacy and security policies and procedures.

    - Technological measures include encryption, removing direct identifiers where possible (and isolation to a separate dedicated server/network where removal is not 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.

    - Physical security includes 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.

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.

In Section 19e) of the COREB application, you will need to 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.

In accordance with the Bruyère Continuing Care Policy (DOC 12), the original master code list may be stored in the Health Information and Client Services Department (formerly known as 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).

3. Length of retention

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.

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

4. Transfer of identifiable data from the source site.

Avoid, where possible, taking data offsite, whether in hard copy or in electronic format.

Section 19f) of the COREB application guidelines, states that data containing personal identifiers should not leave the premises of the research site facility. If data containing personal identifiers will be transferred to another facility, you will need to explain why in this section. In addition, you will need to describe the methods that will be employed to maintain confidentiality of this information 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.

When transporting personal health information in paper format or on removable storage media (CDs, etc.), it must be stored in a locked container, 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:

a. Never leave data unattended or in non-secure locations (e.g., a locked car) as this increases the risk of accidental confidentiality breaches;
b. Ensure computers and files are password protected; and
c. 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.
d. 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.
e. Always exercise extreme caution when using e-mail systems to transfer data. E-mail is not secure. Safe e-mailing procedures are especially important.

5. Destruction/disposal of personal health information.

In order to protect the confidentiality of personal health information, confidential information that is no longer required must be shredded before being recycled.

For CD shredding, Shred-It, a company contracted by the hospital for document shredding, provides such a service.

When computers that contain personal health information are no longer needed, the drives must be cleaned by doing a triple delete (DOC 02, Section 5.2). When you delete information on a hard drive, it is not really deleted - or rather, it can be retrieved. The triple delete process is done by a software called Gdisk from Symantec and it writes zeros on all sectors of the hard drives and does that three times. For more information about using GDisk, see the *Symantec Ghost Reference Guide*.

Triple delete is not the same as defragmenting a drive. Defragmenting re-organizes the data on a drive, which may be spread out all over the drive (fragmented), so that it is more organized. This makes it easier to find data on the drive. Triple deleting deletes the information on the drive