THE UNIVERSITY OF BRITISH COLUMBIA

Research Ethics, Office of Research Services
Suite 102, 6190 Agronomy Road
Vancouver B.C., V6T 1Z3

Phone: 604-827-5112
Fax: 604-822-5093

BREB Policy & Procedure for Breaches in Data Security and Protection of Confidentiality

Background:

In BREB applications and accompanying informed consent forms, researchers describe the nature of their interaction with study participants. This includes a description of how they will fulfill their commitment to maintaining confidentiality of study participants and ensuring the security of research data.

Behavioural researchers employ a variety of research approaches that may include: video-taping, conducting one-to-one interviews in the field, or completing anonymous questionnaires. Because methodologies and study designs differ, procedures used to maintain confidentiality of participants and the security of data will vary considerably. Nevertheless, each investigator must document procedures to be used in each study of their BREB application.

It is BREB's position that a **breach** of confidentiality of study participants, or of the security of research data, has taken place when:

a. there is a failure to conform to the commitment that the investigator made to the study participant, and

b. the failure to conform to the commitment leads to "*a loss of control of study data such that **some or all** of that data has, **or potentially has**, entered the public domain*" (i.e. data has become available, or is potentially available, to any person who is not authorized to view or access the data).

Such situations include, but are not limited to, times when a paper file containing participant identifiers has been lost, a laptop has been stolen, a 'memory stick' has been lost, or audio or video recordings have been misplaced.

Breaches of confidentiality as described constitute an unanticipated event in accordance with REB policies (SOP 405, Articles 3.5 and 3.6) and will be treated by the REB accordingly.

To reduce the likelihood of breaches and to ensure that confidentiality and data security commitments are met the BREB recommends that:

1. Principal Investigators establish policies and procedures to ensure that:

a. all persons who have contact with data (in any form) understand and agree to conform to their ethical responsibilities and the designated procedures for all studies in which they are involved
b. all persons who have contact with data understand what constitutes a 'breach' in confidentiality or data security and how they are to proceed in the event of a breach.
c. A list of all study personnel who will have access to the data be created and kept current;

2. Research labs and/or or research teams have general and specific procedures for:
    a. maintaining confidentiality of data
    b. maintaining security of data (i.e., policies re: storage of laptops or portable electronic data storage devices while in the field, etc.)

3. Principal Investigators require members of the research team to notify them in the event of a breach, or a suspected breach, in confidentiality or security of data.

4. It is expected that in the event of a 'breach' Principal Investigators will file a '**request for acknowledgement**' (this can be done on RISe by creating a '**New Post Approval Activity**'):
    a. notifying BREB that there has been a breach;
    b. describing the conditions of the breach;
    c. outlining the steps that have been taken to address it; and
    d. notifying the privacy officer for the appropriate institution of the breach if the study has been conducted in connection with an institution (e.g. school, hospital, etc).

Procedures that may rectify and contain potential damage from breaches of confidentiality/security include:

a. notification of research participants concerning the nature of the breach
b. containing the breach by terminating access of others to the data
c. containing the breach by obtaining the agreement of a recipient of the data to destroy the data and/or not to transfer or further release the data

In consultation with BREB (Chairs/ or staff) the PI will develop procedures for 'handling the breach' which may include: modifying the procedure for data management; notifying study participants.

For more information please refer to Article 5.1 of the Tri Council Policy Statement which states that: "Breaches of confidentiality may harm the participant, the trust relationship between the researcher and the participant, other individuals or groups, and/or the reputation of the research community".