

[Section 3]

PRIVACY AND CONFIDENTIALITY

Dignity and autonomy of human subjects is the ethical basis of respect for the privacy of research subjects. Privacy is a fundamental value, perceived by many as essential for the protection and promotion of human dignity. Hence, the access, control and dissemination of personal information are essential to ethical research.

Information that is disclosed in the context of a professional or research relationship must be held confidential. Thus, when a research subject confides personal information to a researcher, the researcher has a duty not to share the information with others without the subject's free and informed consent. Breaches of confidentiality may cause harm: to the trust relationship between the researcher and the research subject; to other individuals or groups; and/or to the reputation of the research community. Confidentiality applies to information obtained directly from subjects or from other researchers or organizations that have a legal obligation to maintain personal records confidential. In this regard, a subject-centred perspective on the nature of the research, its aims and its potential to invade sensitive interests may help researchers better design and conduct research. A matter that is public in the researcher's culture may be private in a prospective subject's culture, for example.

There is a widespread agreement about the rights of prospective subjects to privacy and the corresponding duties of researchers to treat private information in a respectful and confidential manner. Indeed, the respect for privacy in research is an internationally recognized norm and ethical standard. It has been enshrined in Canadian law as a constitutional right and protected in both federal and provincial statutes. Model voluntary codes have also been adopted to govern access to, and the protection of, personal information.¹

The values underlying the respect and protection of privacy and confidentiality are not absolute, however. Compelling and specifically identified public interests, for example, the protection of health, life and safety, may justify infringement of privacy and confidentiality. Laws compelling mandatory reporting of child abuse, sexually transmitted diseases or intent to murder are grounded on such reasoning; so too are laws and regulations that protect whistle-blowers. Similarly, without access to personal information, it would be difficult, if not impossible, to conduct important societal research in such fields as epidemiology, history, genetics and politics, which has led to major advances in knowledge and to an improved quality of life. The public interest thus may justify allowing researchers access to personal information, both to advance knowledge and to achieve social goals such as designing adequate public health programs.

Historically, the benefits of the confidential research use of personal data have been substantial. Two of many such examples are: the identification of the relationship between tobacco and lung cancer; and the use of employment or educational records to identify the benefits or harms of various social factors. In the last two decades, larger databases and newer techniques have improved the capacity of researchers to evaluate the delivery of services and the outcomes of many procedures and products. These studies have contributed to more responsive and efficient service delivery in areas such as health, education, safety and the environment.

Ethics review is thus an important process for addressing this conflict of societal values. The REB plays an important role in balancing the need for research against infringements of privacy and minimizing any necessary invasions of privacy. Individuals should be protected from harm caused by unauthorized use of personal information in which they believed they had an expectation of privacy and the benefit of confidentiality.

The situation may arise where a third party attempts to gain access to research records, and hence to breach the promise of confidentiality given by the researcher as part of a research project approved by the REB. By that time, the matter has passed from the hands of the REB. The researcher is honour-bound to protect the confidentiality that was undertaken in the process of free and informed consent, to the extent possible within the law. The institution should normally support the researcher in this regard, in part because it needs to protect the integrity of its own REB. If the third party attempts to secure the research data by subpoena, it is legitimate for the researcher and the institution to argue the issue in court. The records of the REB and of the consent might be useful as part of this counter-argument, or may be requested by those seeking access. However, if the court issues a subpoena, legal appeals will probably be the only legal option open to the researcher to protect the confidentiality of the records.

In the process of free and informed consent, researchers should indicate to research subjects the extent of the confidentiality that can be promised, and hence should be aware of the relevant law.

The articles below articulate the general rule to protect privacy and confidentiality through notification and consent of the individuals whose personal information is involved. For the purposes of this Policy, identifiable personal information means information relating to a reasonably identifiable person who has a reasonable expectation of privacy. It includes information about personal characteristics such as culture, age, religion and social status, as well as their life experience and educational, medical or employment histories. However, Article 1.1(c) excludes from REB review research that is based exclusively on publicly available information. This includes documents, records, specimens or materials from public archives, published works and the like, to which the public is granted access.

As a general rule, the best protection of the confidentiality of personal information and records will be achieved through anonymity. If the data being stored are truly anonymous, the research project will need only minimal REB scrutiny.

A. Accessing Private Information: Personal Interviews

Article 3.1 **Subject to the exceptions in Article 1.1(c), researchers who intend to interview a human subject to secure identifiable personal information shall secure REB approval for the interview procedure used and shall ensure the free and informed consent of the interviewee as required in Article 2.4. As indicated in Article 1.1, REB approval is not required for access to publicly available information or materials, including archival documents and records of public interviews or performances.**

Article 3.1 requires REB approval for collection of information through personal interviews, which may be described as including such means as face-to-face, telephone or other electronic encounters, or individualized questionnaires, that the researcher uses to gather materials for such purposes as a biographical study or other research involving specific personalities. To assist the review of such activities, REBs may wish to encourage faculties and departments that use individual interviews extensively to develop standard interview procedures based on Article 2.3 and Article 3.1, as well as on the requirements of their professional organizations, if they so wish. Prior approval of such interview procedures may greatly simplify further review of similar protocols, though the dangers of attempting to enforce a single interview procedure on the varied circumstances within a complex institution are evident.

The task of the REB is to ensure that individuals who are approached for interviews are given the information required by this Policy in order to be able to give free and informed consent. It is clear that individuals have the right to refuse to be interviewed, if they so wish.

Nothing in this article should be interpreted to mean that REBs should engage in prior censorship of research concerning those in the public arena or in artistic and literary life (see Article 1.1(c)).

B. Accessing Private Information: Surveys, Questionnaires and the Collection of Data

Article 3.2 **Subject to Article 3.1 above, researchers shall secure REB approval for obtaining identifiable personal information about subjects. Approval for such research shall include such considerations as:**

- (a) The type of data to be collected;**
- (b) The purpose for which the data will be used;**
- (c) Limits on the use, disclosure and retention of the data;**
- (d) Appropriate safeguards for security and confidentiality;**
- (e) Any modes of observation (e.g., photographs or videos) or access to information (e.g., sound recordings) in the research that allow identification of particular subjects;**
- (f) Any anticipated secondary uses of identifiable data from the research;**
- (g) Any anticipated linkage of data gathered in the research with other data about subjects, whether those data are contained in public or personal records; and**
- (h) Provisions for confidentiality of data resulting from the research.**

Article 3.2 requires researchers to secure REB review before commencing research involving identifiable personal information collected from subjects by such means as interviews, questionnaires, observation, access to private files or records, etc.

Researchers should ensure that the data obtained are stored with all the precautions appropriate to the sensitivity of the data. Data released should not contain names, initials or other identifying information. While it may be important to preserve certain types of identifiers (e.g., region of residence), these should be masked as much as possible using a standardized protocol before the data are released for research purposes. However, legitimate circumstances may exist where such information is critical for the research project. Accordingly, information that identifies individuals or groups should be kept in different databases with unique identifiers. Researchers should take reasonable measures to ensure against inadvertent identification of individuals or groups, and must address this issue to the satisfaction of the REB.

Article 3.2 states that subjects have a right to know who will have access to identifying information, and to know about the nature of that information. In particular, the researcher should inform the subject if the information will be provided to the government, government agencies, personnel from an agency that monitors the research, the research sponsor (e.g., a pharmaceutical company), the REB or a regulatory agency. This would also include situations in which mandatory reporting is required, such as under laws requiring reporting of child abuse, infectious diseases or homicidal intent. The REB and the researcher should be sensitive to the interests of those who might suffer from stigmatization. For example, when records of prisoners, employees, students or others are used for research purposes, the researcher should not provide authorities with results that could identify individuals, unless the prior written consent of the subjects is obtained. Researchers may, however, provide to administrative bodies, for policy decision making purposes, aggregated data that cannot be linked to individuals.

Article 3.2 refers not only to the secondary uses of information in research, but also for other purposes, such as the subsequent use of research videos for educational purposes. It is essential that subsequent uses of data be specified in sufficient detail that prospective subjects may give free and informed consent; it is inappropriate to seek blanket permission for “research in general.”

Article 3.2(g) is important because information that may on its own be seen as innocuous by the subject may take on a completely different meaning if linked to other data (see Article 3.6).

C. Secondary Use of Data

Secondary use of data refers to the use in research of data contained in records collected for a purpose other than the research itself. Common examples are patient or school records or biological specimens, originally produced for therapeutic or educational purposes, but now proposed for use in research. This issue becomes of concern only when data can be linked to individuals, and becomes critical when the possibility exists that individuals can be identified in the published reports.

Article 3.3

If identifying information is involved, REB approval shall be sought for secondary uses of data. Researchers may gain access to identifying information if they have demonstrated to the satisfaction of the REB that:

- (a) Identifying information is essential to the research;**
- (b) They will take appropriate measures to protect the privacy of the individuals, to ensure the confidentiality of the data, and to minimize harms to subjects; and**
- (c) Individuals to whom the data refer have not objected to secondary use.**

Databases can vary greatly in the degree to which personal information is identifiable. A proportionate approach should be applied by the REB to evaluate the sensitivity of the information in the database and to modulate its requirements accordingly. If it is impossible to identify individuals whose records exist within a database, then researchers should be allowed access to that database. The REB must carefully appraise the possibility of identification, in particular with regard to the extent of the harm or stigma that might be attached to identification. The REB and the researcher should also be aware of legal provisions that affect the database(s) to be used in the research.

REBs and researchers should also be sensitive to the context in which the database was created, such as a confidential relationship, as well as to the expectations of the groups or individuals at the time of the collection of the data with regard to its use, retention and disclosure. When it is unclear as to whether information is to be regarded as personal, researchers should consult their REBs. Confidential information collected in this manner should normally not be transmitted to authorities, unless required by law, the courts or similar legally constituted bodies.

Article 3.4

The REB may also require that a researcher's access to secondary use of data involving identifying information be dependent on:

- (a) The informed consent of those who contributed data or of authorized third parties; or**
- (b) An appropriate strategy for informing the subjects; or**
- (c) Consultation with representatives of those who contributed data.**

Article 3.4 is based on the concept of a proportionate approach to ethical assessment of research. Under it, the REB should focus on projects above minimal risk, or modulate requirements and protection proportionate to the magnitude and probability of harms, including the likelihood that published data can be linked to individuals. In highly sensitive situations, such as when identifiable data will be published or other instances when there is a significant risk of breach of confidentiality, Article 3.4(a) indicates that such deliberations and balancing may lead the REB to seek consent to use the stored data from those who made the contribution.

It may be impossible, difficult or economically unfeasible to contact all subjects in a study group to obtain informed consent. This can occur when the group is large or its members are deceased, geographically dispersed or difficult to track. In such cases, Article 3.4(b) requires that the researcher propose an appropriate strategy for informing the relevant parties or, in accord with Article 3.4(c), that there be consultation with representative members of the affected group (e.g., in an AIDS study, contacting one or a number of AIDS advocacy groups), or that there be some way to sample the opinions of a subset of individuals in the group.

Article 3.5 Researchers who wish to contact individuals to whom data refer shall seek the authorization of the REB prior to contact.

In certain cases, the research goal may only be achieved by follow-up contact and interviews with persons. It is evident that individuals or groups might be sensitive if they discover that research was conducted on their data without their knowledge; others may not want any further contact. This potential harm underlines the importance for researchers to make all efforts to allow subjects the right to consent that their data and private information be part of a study.

D. Data Linkage

Article 3.6 The implications of approved data linkage in which research subjects may be identifiable shall be approved by the REB.

Advances in our abilities to link databases create both new research opportunities and new threats to privacy. These techniques may provide avenues for addressing previously unanswerable questions and for generating better social and health-related information. The values underlying the ethical obligation to respect privacy oblige researchers and REBs to exercise caution in the creation and use of data of this kind. REBs should also be aware of relevant statutory frameworks, and the criteria required by government for authorization of use of data in governmental data banks.² Only a restricted number of individuals should perform the function of merging databases; researchers should either destroy the merged file immediately after use, or use enhanced security measures to store it. Whether the data are to be used statistically or otherwise, confidentiality of the information must be maintained by all members of the research team. When a merged database identifies a person or a group who might be at significant risk of harm, it may be appropriate to contact those at risk or the appropriate authorities. The REB and the record holder should also be notified.

End notes

¹ Canadian Standards Association, *Model Code for the Protection of Personal Information*. 1996.

² See *Statistics Act*, Revised Statutes of Canada. 1985, chapter S-19.