





their personal characteristics such as culture, age, religion and social status, as well as their life experience and educational, medical, or employment histories.

These guidelines exclude the REB from reviewing 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.

## B. ACCESSING PRIVATE INFORMATION: PERSONAL INTERVIEWS

1. Researchers who intend to interview a human subject to secure identifiable personal information must secure REB approval for the interview procedure used and shall ensure the free and informed consent of the interviewee.
2. REB approval is not required for access to publicly available information or materials, including archival documents and records of public interviews or performances

- 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.

When research involves accessing private information, researchers must ensure the following:

### **1. Securing REB Review**

Researchers are required 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.

### **2. Storing of Data**

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 identifi



