MPHEC
Maritime Provinces
Higher Education
Commission

CESPM
Commission de
l'enseignement supérieur
des Provinces maritimes

The Council of Maritime Premiers
Le Conseil des premiers ministres
des Maritimes

Maritime Provinces Higher Education Commission
Standard for Maintaining Confidentiality

Purpose

To protect the confidentiality of MPHEC data that are individually identifying (directly or indirectly). MPHEC data refer to data collected and/or maintained by MPHEC, including, but not limited to:

- USIS (University Student Information System);
- ESIS (Enhanced Student Information System);
- MPHEC Graduate Survey Databases

Standard

Staff will monitor the confidentiality of personal identification information in their daily activities and in the release of information to the public, following the principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information. The summary of Model Code principles may be found in Attachment 1.

Legal Requirements

Protection of confidentiality of personal identification information collected and/or maintained by the MPHEC is covered by the Maritime Provinces Higher Education Commission Act. This Act, however, is not in force. ESIS data are cleaned and compiled by the MPHEC for Statistics Canada, and are therefore covered by the Statistics Act.

Procedures

Compliance with the Standard is the responsibility of the Chief Executive Officer of the MPHEC. In order to maintain confidentiality for MPHEC data collections, the following conditions must be met:

GENERAL

1. Retention

Due to the archival nature of the databases maintained at the MPHEC, data containing personal identification information will be retained indefinitely.

With respect to the MPHEC graduate survey, lists of graduates containing personal identification information are collected from the participating institutions in order to contact the graduates for followup interviews. For each graduating class, these original contact lists will be destroyed at the end of each survey cycle (i.e., upon release of the five-year-out survey final report).

2. Access to data

ESIS/USIS: Encrypted data files from each institution are received by the MPHEC via a proprietary file transfer protocol (for further information, see MPHEC Local Area Network document). This program encrypts the .txt files using an encryption algorithm known only to the MPHEC. Once the files have been downloaded and decrypted, they are stored under password protection. Once these working files are finalized, the original files a recorded on password-protected CD-ROMs, with one copy stored in a locked cabinet on site, and a second stored off-site in a safety deposit box. The finalized versions are stored on a separate server.

Only those employees carrying out the duties of programming or database administration have access to the full ESIS database including files which contain personal identification information. Access by researchers to the ESIS database excludes these files.

Access to, and release of personally identifying data from, the ESIS database is restricted to the following purposes:

1) To compile a student/graduate contact list for an MPHEC survey,
2) To meet legal requirements
3) Communication with institutions during the ESIS data validation process and with Statistics Canada

MPHEC Graduate Surveys: Survey data will be stripped of direct student identifiers and access will be restricted to employees charged with data analysis and database administration. The data file containing direct student identifiers will be maintained in encrypted format or password - protected on CD-ROM. As with the ESIS original data, access to the secured survey data will be permitted only for the purposes listed above; in addition, the data may also be accessed to verify the accuracy of longitudinal data.

ESIS data validation process: The collection of ESIS data from institutions incorporates a validation process whereby the MPHEC audits the data and works closely with the institutions in cleaning the data. In addition, as part of the MPHEC's mandated function to provide ESIS data collected from Maritime institutions to Statistics Canada, the MPHEC corresponds with Statistics Canada regarding the data. In both cases, the MPHEC staff member carrying out database administration is often required to communicate using student i.d. numbers and other personal identifiers as references. In all instances where this occurs, the MPHEC sends personally identifying data by secure FTP (file transfer protocol).

3. Informing Survey Respondents

Respondents to MPHEC surveys must be informed of the following: objective of survey, proposed use of information provided, protection of data, and data sharing agreements.

4. Record Linkage

A record linkage is defined as the merging of two or more MPHEC micro-records from different databases or surveys to form a composite record. A micro-record is defined as containing information about an individual respondent or unit of observation. Where any record linkage activity is proposed that involves linking existing records (i.e., ESIS data) to information the MPHEC would collect directly from respondents (i.e., the graduate follow-up survey), they must

be notified of the proposed linkage activity at the time of collection. Consent to linking their survey responses to their student record in ESIS would be obtained; they would also be informed of the purpose of the linkage and the value of the resulting information.

Both MPHEC staff and contractors must employ methods in data collection and analysis that protect the confidentiality of personal identification information. Among other things, this means that data files, questionnaires, and other reports having personal data on individuals must be kept secure at all times through the use of passwords, separation of individual identity from the rest of the data, and secure data handling and storage.

RELEASE & DISSEMINATION

Non-Personally Identifying Data

These data do not reveal specific information about a particular individual; they usually describe a group of persons (i.e., aggregate enrolment data) without identifying any one individual. Alternatively, they may consist of individual records stripped of any information that would make it possible to identify the person described.

5. Microdata Release

In reporting on surveys and preparing public/institutional use data files (anonymized files containing individual records from respondents), the goal is to have an acceptably low probability of identifying individual respondents. It is important to be aware of the possibility of inadvertently disclosing personally identifying information even when there is more than a single record in a category.

a) The review and disclosure of public-use data files ensures that, even though the records are at an individual level, they are still not identifying. In preparing files for release to the public, the files must undergo a disclosure analysis. Any modifications that are necessary as a result of the analysis must be made, and the entire process must be documented.

b) For public use data files, one must consider any variables proposed for inclusion on the file that are unusual (such as very high salaries) and data sources that may be available in the public or private sector for matching purposes.

Personally Identifying Data

These data may or may not identify a person directly, but contain information that would make an individual's identity and any related information about them easily recognized, for example, name, address, telephone, SIN or student number (unique student identifier).

6. All MPHEC staff, without exception, have pledged not to release, for any purpose, to any person not sworn to the preservation of confidentiality, any personal identification data. Personal identification data are confidential and protected from legal process unless the individual provides written consent.

7. All contractors whose activities might involve contact with personal identification data shall provide MPHEC project officers with a list of staff who might have contact with such data, together with signed confidentiality agreements for each individual. These agreements will be kept current as new staff are assigned to MPHEC projects with personal identification data.

8. At the discretion of the CEO of the MPHEC, staff may release personal identification data to persons for statistical uses (i.e., contractors executing longitudinal surveys) compatible with the purposes for which the data were collected if those persons sign confidentiality agreements and meet such other requirements as deemed necessary.

9. The release of such data to researchers outside the MPHEC should be considered as a loan of data (recipients do not have ownership of the data), and it should be returned or copies destroyed once the researchers complete their work.

10. When data is released outside the MPHEC, recipients should be required to sign an affidavit stating they will use data in a way consistent with that described in the information request and will not transfer or re-release data to another individual or organization.

ACCESS TO INFORMATION

ESIS

11. Informing students of the objectives of ESIS data collection and provision of the option to opt out of the data collection is the responsibility of Statistics Canada together with the individual institutions.

12. Upon request by a student, Statistics Canada will delete personal contact information (name, address, telephone number, SIN, ESIS_NSN, e-mail) from the ESIS database. The removal of this information will make it impossible for users to identify this/these individual(s). The MPHEC will be informed of any changes by Statistics Canada. Students who wish to make such as request must contact Statistics Canada:

Via Mail:	Postsecondary Education and Adult Learning Section Centre for Education Statistics Statistics Canada, Jean Talon Building, 1-B-9 Tunney's Pasture, Ottawa, Ontario, K1A 0T6
Via Telephone:	Monday to Friday: 8:00 A.M.. - 5:00 P.M. EST/EDST 1-613-951-1666
Via E-mail:	ESIS-SIAE_contact@statcan.ca
Source:	http://www.statcan.ca/english/concepts/ESIS/contacts.htm

The Privacy Act provides individuals with a right of access to their personal information held by the federal government. Students may request to see their personal information in the Enhanced Student Information System using the contact information above.

13. Individuals have the right to access their records, to ensure that the information is accurate. Individuals wishing to do so must make the request through their institution. Any changes to be made to ESIS records will be forwarded to the MPHEC by the institution.

14. Institutions have the right to access their records, to ensure that the information is accurate. The MPHEC will provide access, if deemed reasonable, upon receipt of a written request, stating the nature and purpose of the request, the reason for concern about the accuracy of the records, and the records to be accessed.

Revised version on February 9, 2004

Attachment 1

CSA Model Code for the Protection of Personal Information

Many Canadian companies have implemented voluntary codes to safeguard their customers' privacy rights. Such codes are based on the premise that clients' personal information should not be misused, and that individuals should have access to their own personal information.

In 1996, the Canadian Standards Association (CSA) developed a voluntary code based on the work of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, created by the international Organization for Economic Cooperation and Development (OECD). The CSA's version, its Model Code for the Protection of Personal Information, has been endorsed by many Canadian companies as the national standard on privacy protection.

The ten basic principles of the Code are:

1.	Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2.	Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3.	Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4.	Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5.	Limiting Use, Disclosure and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6.	Accuracy	Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.
7.	Safeguards	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8.	Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9.	Individual Access	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10.	Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.