# Income Security Program (ISP)
# Data Matching/Sharing - Security of Information & Privacy

## Policy Guidelines and Audit Framework

In February of 1998 a review of all agreements ISP currently has concerning the sharing of information with the provinces and other federal agencies and programs was conducted. In all instances, it was reported that only those elements of personal information that must be disclosed in accordance with the relevant authority to do so was in fact given. Furthermore, in no cases was a complete copy of the databases provided.

The TB manual for Privacy and Data Protection volume provides a set of guidelines for the sharing of data and data matching programs. Benefits could be derived from developing a policy which will document what information may be shared and under what circumstances. Such a policy would help safeguard the personal information under ISPs control, at the same time such the policies and subsequent agreements would provide a framework which would enable a compliance audit to be conducted should one be required.

For the purpose of this document:

Data - is a set or sets of records containing information

Matching Program - is a specific procedure that is developed and used to compare data from one institution with data from another.

Information - is the product generated by a matching program

## Policy with Respect to an Audit Framework

*Internal Issues for ISP:*

- The creation of a data dictionary which indicates each unique data field in all of ISPs systems and databases would be a useful resource for future agreements. For optimum benefit the data obtained from other government departments such as Canada Customs and Revenue Agency should also be included in the dictionary. Information of use in such a dictionary would be who the owner of the data is, which data elements may be shared, to whom and under what circumstances. For example, a case may arise that if a particular data element is identified as being sharable then in so choosing that item you may cause another sharable item to become non sharable. In other words, data items A and B are both sharable, however both A and B cannot be shared in the same match program. This dictionary could prove to be a useful tool in an audit.

- It is the policy of the government to prevent the SIN from becoming a universal identifier. However, provincial governments have been legislated to use the SIN in delivering programs and services.  This has resulted in the SIN being used as the link field in many data match programs.  These factors must be weighed when requested to provide the SIN number as a pure data element. Reference can be made to the TB manual on Privacy and Data Protection volume and to the Report of the Auditor General of Canada Chapter 16 September 1998 in particular 16.25 - 16.28.

- Since 1976, when the first data sharing agreement was entered into the collection, retention and distribution methods for such data has undergone tremendous change.  ISP may wish to consider alternative methods in light of the technology available today.  Some alternative methods include:

  ⇒ Providing access to our data by the Internet and employing security techniques such as Public Key Infrastructure (PKI).  PKI is a method which allows the access to encrypted by providing a decryption key which must be matched with the host to allow for decryption;

  ⇒ Having the client provide us with their data, allowing us to conduct the match;

  ⇒ Providing a real time link to our mainframe systems for interactive searches as Insurance is doing with a limited number of screens.

*External Issues for ISP:*

- The organization who wishes to conduct a data match program must state the purpose of the match program and demonstrate that the program is directly related to an activity or operating program of the organization. The organization must show how they plan to use the data being shared.  This should include what data elements they plan to do a match on and what the intended results will be.  The match program and use of the data should be subject to approval by ISP prior to releasing the data. TB manual - Privacy and Data Protection volume 2-5 Data Matching (b)  This requirement should be built into the agreement between ISP and the organization wishing to establish a matching program.

- The agreement should contain a clause which restricts the data obtained under one agreement from being used or linked in any way with the data obtained by the same organization under a separate agreement. Should such an event occur, this could potentially violate the policy on the use of personal information, limiting the use of such information for the purposes for which it was obtained.  Reference to the Privacy Act; TB manual - Privacy and Data Protection 2-4 (1-2).

- Only the information that is being requested and is deemed necessary for the match program should be provided to the organization requesting the information.  As stated in the HRDC Profile of Personal Information Collection, Use and Disclosure Report of 1998, this is being done however, any policy directive should re-emphasize this fact.

- The agreement should contain a clause which states that the data being shared is for a specific data match program and should be considered to remain under ISPs ownership. The agreement should restrict the contractee from further distribution or sharing of the data being requested. As mentionned above, further sharing of the data could violate the Privacy Act restricting the use of personal information for the purpose in which it was collected. TB manual 2-04-2.

- It should be established who the owner of the information is once the match is completed, for example ISP, the other organization or jointly. It should be stated in the agreement if the generated information can be shared, and if so to whom and under what circumstances it can be shared. Although we did not link this to any specific clause in the TB manual or Privacy Act, it is our opinion that this is the intent of the guidelines as outlined in the TB manual.

- The details of the match program must indicate the start and completion dates of the match program and indicate if any updates to the data being used will be required, and if so, at what intervals the updates will occur. This will ensure the data is up to date and is used effectively. TB manual - 2-5 (g). This will enable the monitoring of the match program and assist in the detection of any potential misuses by providing a clear time line which can be used in an audit.

- A time frame should be established in all agreements which will allow for the cancellation of or automatic review of the agreement on a routine basis. This built in monitoring feature will help to ensure that complacency does not occur over time regarding the sharing of information. This will also allow for changes in the match program to occur based on changing technology.

- A clause should be included in the agreements which will allow for the Minister to appoint a mutually acceptable Auditor to periodically conduct reviews and audits.

- It should be determined to what extent the regulations pertaining to the retention and subsequent disposal of the data could and should apply to the shared data. A provision which states what these regulations are should be included in the agreement. TB manual 2-03.

**Income Security Programs (ISP) Data Matching/Sharing -**
**Security of Information & Privacy**

Request: Assistance in developing related policies and guidelines and establishing an audit framework.

Background: Since 1976, ISP has entered into 30 information sharing agreements.

Many agreements have not been reviewed since signed, nor do they have a termination clause.

ISP is concerned about sharing sensitive information or information obtained from other sources such as Canada Customs and Revenue Agency (CCRA), formerly known as Revenue Canada.

Ontario implemented a co-payment program for prescription drugs based on income. Eleven residents claimed that ISP had passed on CCRA information to the province. Although this was not the case, the program had to be terminated.

Solutions: Analysis of current policies with respect to privacy, data match programs and access to information.

Development of recommendations based on internal and external ISP issues.

Details:

Internal: Creation of a data dictionary:

- Owner of data;
- Which elements may be shared;
- With whom;
- Conditions.

Awareness of the use of the social insurance number (SIN) and the Office of the Auditor General of Canada (OAG) report.

Alternatives to data sharing were suggested given advancement in technology since 1976:

- Public key infrastructure (PKI);
- ISP conducting data match with client supplied data;
- Limited direct access to our databases.

External: Development of a well written agreement stating:

- Purpose of the match program;
- How the request is directly related to their operations;

- Data shared under one agreement may not be shared with data from another match program;
- Shared data remains under the ownership of ISP;
- the Minister may appoint a mutually acceptable auditor.

The owner of the information derived from the match program and the potential use of such information should be disclosed prior to signing a data sharing agreement.

Issues pertaining to the retention and disposal of the shared data should be assessed for both federal and provincial compliance.

Outcome: Positive acceptance of the report.

Many points were new to ISP such as the creation of the data dictionary

Other points provided assurance that ISP was proceeding in the right direction.

Project was deemed complete however the door was left open if further information is needed at a later date.

**Policy Objectives - Privacy and Data Protection**

It is the policy of the government:

◊ to account for and give public notice of data matching carried out by or on behalf of the government; and

◊ to prevent the SIN from becoming a universal identifier by:

- limiting collection and use of the SIN by institutions to specific acts, regulations and programs, and

- notifying individual clearly as to the purposes for collecting the SIN and whether any right, benefit or privilege could be withheld or any penalty imposed if the number is not disclosed to the federal institution requesting it.

***Chapter 1***

**Policy Requirements**

Use of the Social Insurance Number

17.1 limit their uses of the Social Insurance Number (SIN) for administrative purposes to those authorized by statute or regulation and for administering pensions, income tax, health and social programs (as listed in Chapter 3-4).

17.4 when the SIN is included in any personal information bank, so indicate in the description of the bank provided for Info Source and cite the authority under which the number is collected and the purpose for which it is used.

***Chapter 2***

**Use and Disclosure of Personal Information**

Provinces, foreign states and international bodies

6.6 … information may be disclosed under an agreement … between the Government of Canada … and the government of a province … or any institution of any such government or organization, for the purpose of administering or enforcing any law …

… this permits federal government institutions to disclose personal information …for the purpose of administering a statute … Examples of this type of disclosure include the federal-provincial exchange of information related to social assistance…

Disclosures …are to be made…with a formal written agreement…these agreements must contain the components listed in Chapter 3-5.