

Government of Saskatchewan Privacy Assessment

February 12, 2003



Table of Contents

EXECUTIVE SUMMARY	7
POTENTIAL NEXT STEPS	10
RECOMMENDATIONS	13
OBJECTIVES.....	16
LIMITATIONS.....	17
EVOLVING ROLE OF PRIVACY IN CANADA	19
THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT	22
COMPARISON TO OTHER CANADIAN JURISDICTIONS	23
CANADIAN STANDARDS ASSOCIATION PRIVACY PRINCIPLES.....	25
PRINCIPLE 1 - ACCOUNTABILITY	26
OVERVIEW OF THE GOVERNMENT OF SASKATCHEWAN.....	27
PRINCIPLE 2 - IDENTIFYING PURPOSES	29
OVERVIEW OF THE GOVERNMENT OF SASKATCHEWAN.....	30
PRINCIPLE 3 - CONSENT	32
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	34
PRINCIPLE 4 - LIMITING COLLECTION.....	37
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	37
PRINCIPLE 5 - LIMITING USE, DISCLOSURE AND RETENTION.....	39
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	39
PRINCIPLE 5 - LIMITING USE, DISCLOSURE AND RETENTION (CONTINUED).....	40
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN (CONTINUED)	40
PRINCIPLE 6 - ACCURACY	41
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	41
PRINCIPLE 7 - SAFEGUARDS	43
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	43
PRINCIPLE 8 - OPENNESS.....	47
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	47
PRINCIPLE 9 - INDIVIDUAL ACCESS	49
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	50
PRINCIPLE 10 - CHALLENGING COMPLIANCE.....	52
OVERVIEW OF GOVERNMENT OF SASKATCHEWAN	52
PRINCIPLE 10 - CHALLENGING COMPLIANCE (CONTINUED).....	53
APPENDICES.....	54
APPENDIX A - INFORMATION BY DEPARTMENT OR CROWN CORPORATION.....	54
1. SASKATCHEWAN AGRICULTURE, FOOD AND RURAL REVITALIZATION (SAFRR).....	55



- INTRODUCTION 55
- ACCOUNTABILITY 56
- IDENTIFYING PURPOSES 57
- CONSENT 58
- LIMITING COLLECTION 58
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 58
- MAINTAINING ACCURACY 59
- SAFEGUARDS 59
- OPENNESS 59
- PROVIDING ACCESS 60
- CHALLENGING COMPLIANCE 60
- RECOMMENDATIONS 61
- 2. CORRECTIONS AND PUBLIC SAFETY 63**
- INTRODUCTION 63
- ACCOUNTABILITY 63
- IDENTIFYING PURPOSES 64
- CONSENT 65
- LIMITING COLLECTION 66
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 66
- MAINTAINING ACCURACY 66
- SAFEGUARDS 67
- OPENNESS 68
- PROVIDING ACCESS 68
- CHALLENGING COMPLIANCE 69
- RECOMMENDATIONS 69
- 3. SASKATCHEWAN ENVIRONMENT 71**
- INTRODUCTION 71
- ACCOUNTABILITY 72
- IDENTIFYING PURPOSES 73
- CONSENT 75
- LIMITING COLLECTION 76
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 76
- MAINTAINING ACCURACY 77
- SAFEGUARDS 78
- OPENNESS 78
- PROVIDING ACCESS 79
- CHALLENGING COMPLIANCE 80
- RECOMMENDATIONS 80
- 4. FINANCE 82**
- INTRODUCTION 82
- ACCOUNTABILITY 83
- IDENTIFYING PURPOSES 85
- CONSENT 86
- LIMITING COLLECTION 88
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 88
- MAINTAINING ACCURACY 89
- SAFEGUARDS 89
- OPENNESS 91
- PROVIDING ACCESS 91
- CHALLENGING COMPLIANCE 92



RECOMMENDATIONS	93
5. HEALTH	95
INTRODUCTION	95
ACCOUNTABILITY	98
IDENTIFYING PURPOSES	100
CONSENT	103
LIMITING COLLECTION	105
LIMITING USE, DISCLOSURE, COLLECTION & RETENTION	105
MAINTAINING ACCURACY	106
SAFEGUARDS	107
OPENNESS	108
PROVIDING ACCESS	108
CHALLENGING COMPLIANCE	109
RECOMMENDATIONS	109
6. HIGHWAYS & TRANSPORTATION	111
INTRODUCTION	111
ACCOUNTABILITY	112
IDENTIFYING PURPOSES	112
CONSENT	113
LIMITING COLLECTION	113
LIMITING USE, DISCLOSURE, COLLECTION & RETENTION	113
MAINTAINING ACCURACY	114
SAFEGUARDS	114
OPENNESS	115
PROVIDING ACCESS	115
CHALLENGING COMPLIANCE	116
RECOMMENDATIONS	116
7. INFORMATION SERVICES CORPORATION	118
INTRODUCTION	118
ACCOUNTABILITY	120
IDENTIFYING PURPOSES	122
CONSENT	124
LIMITING COLLECTION	124
LIMITING USE, DISCLOSURE, COLLECTION & RETENTION	125
MAINTAINING ACCURACY	126
SAFEGUARDS	126
OPENNESS	126
PROVIDING ACCESS	127
CHALLENGING COMPLIANCE	128
RECOMMENDATIONS	128
8. JUSTICE	130
INTRODUCTION	130
ACCOUNTABILITY	131
IDENTIFYING PURPOSES	133
CONSENT	134
LIMITING COLLECTION	135
LIMITING USE, DISCLOSURE, COLLECTION & RETENTION	135
MAINTAINING ACCURACY	136
SAFEGUARDS	136



- OPENNESS 137
- PROVIDING ACCESS 137
- CHALLENGING COMPLIANCE 138
- RECOMMENDATIONS 138
- 9. LEARNING 141**
- INTRODUCTION 141
- ACCOUNTABILITY 145
- IDENTIFYING PURPOSES 149
- CONSENT 153
- LIMITING COLLECTION 155
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 156
- MAINTAINING ACCURACY 157
- SAFEGUARDS 158
- OPENNESS 159
- PROVIDING ACCESS 160
- CHALLENGING COMPLIANCE 162
- RECOMMENDATIONS 163
- 10. SASKENERGY 165**
- INTRODUCTION 165
- ACCOUNTABILITY 165
- IDENTIFYING PURPOSES 166
- CONSENT 167
- LIMITING COLLECTION 168
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 168
- MAINTAINING ACCURACY 168
- SAFEGUARDS 169
- OPENNESS 169
- PROVIDING ACCESS 169
- CHALLENGING COMPLIANCE 171
- RECOMMENDATIONS 171
- 11. SASKPOWER 173**
- INTRODUCTION 173
- ACCOUNTABILITY 173
- IDENTIFYING PURPOSES 175
- CONSENT 176
- LIMITING COLLECTION 176
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 176
- MAINTAINING ACCURACY 176
- SAFEGUARDS 177
- OPENNESS 177
- PROVIDING ACCESS 178
- CHALLENGING COMPLIANCE 178
- RECOMMENDATIONS 179
- 12. SASKATCHEWAN LIQUOR AND GAMING AUTHORITY 180**
- INTRODUCTION 180
- ACCOUNTABILITY 183
- IDENTIFYING PURPOSES 185
- CONSENT 186
- LIMITING COLLECTION 187



- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 188
- MAINTAINING ACCURACY 188
- SAFEGUARDS 189
- OPENNESS 190
- PROVIDING ACCESS 190
- CHALLENGING COMPLIANCE 191
- RECOMMENDATIONS 192

- 13. SASKATCHEWAN PROPERTY MANAGEMENT CORPORATION 193**
- INTRODUCTION 193
- ACCOUNTABILITY 194
- IDENTIFYING PURPOSES 196
- CONSENT 196
- LIMITING COLLECTION 196
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 197
- MAINTAINING ACCURACY 197
- SAFEGUARDS 197
- OPENNESS 198
- PROVIDING ACCESS 198
- CHALLENGING COMPLIANCE 199
- RECOMMENDATIONS 199

- 14. SASKTEL 201**
- INTRODUCTION 201
- ACCOUNTABILITY 201
- IDENTIFYING PURPOSES 202
- CONSENT 202
- LIMITING COLLECTION 202
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 202
- MAINTAINING ACCURACY 203
- SAFEGUARDS 203
- OPENNESS 203
- PROVIDING ACCESS 203
- CHALLENGING COMPLIANCE 204
- RECOMMENDATIONS 204

- 15. SGI 206**
- INTRODUCTION 206
- ACCOUNTABILITY 207
- IDENTIFYING PURPOSES 208
- CONSENT 209
- LIMITING COLLECTION 210
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 210
- MAINTAINING ACCURACY 212
- SAFEGUARDS 212
- OPENNESS 213
- PROVIDING ACCESS 213
- CHALLENGING COMPLIANCE 214
- RECOMMENDATIONS 215

- 16. SASKATCHEWAN HEALTH INFORMATION NETWORK (SHIN) 217**
- INTRODUCTION 217
- ACCOUNTABILITY 217



- IDENTIFYING PURPOSES 218
- CONSENT 218
- LIMITING COLLECTION 219
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 219
- MAINTAINING ACCURACY 219
- SAFEGUARDS 219
- OPENNESS 220
- PROVIDING ACCESS 220
- CHALLENGING COMPLIANCE 220
- RECOMMENDATIONS 220

- 17. SOCIAL SERVICES..... 221**
- INTRODUCTION 221
- ACCOUNTABILITY 231
- IDENTIFYING PURPOSES 234
- CONSENT 237
- LIMITING COLLECTION 240
- LIMITING USE, DISCLOSURE, COLLECTION & RETENTION 240
- MAINTAINING ACCURACY 241
- SAFEGUARDS 242
- OPENNESS 243
- PROVIDING ACCESS 244
- CHALLENGING COMPLIANCE 247
- RECOMMENDATIONS 248

- APPENDIX B..... 250**

Executive Summary

In June, 2002 the Government of Saskatchewan, Executive Council asked Deloitte and Touche to perform a high level review of the information privacy policies, procedures, controls and systems in place at 17 selected government departments and Crown Corporations as a result of publicized concerns regarding the protection of personal information housed by departments and Crown Corporations. The 17 departments and Crown Corporations were:

- Agriculture, Food and Rural Revitalization
- Corrections and Public Safety
- Environment
- Finance
- Health
- Highways & Transportation
- Information Services Corporation
- Justice
- Learning
- SaskEnergy
- SaskPower
- Saskatchewan Liquor and Gaming Authority
- Saskatchewan Property Management Corporation
- Sask Tel
- SGI
- Saskatchewan Health Information Network (SHIN)
- Social Services

The Government of Saskatchewan has begun to research how current day privacy practices should be incorporated into existing frameworks, which protect personal information, and to assess whether any changes are required. The primary purpose of this study was to help ascertain the existing level of attention given to privacy within the Government by assessing the personal information management practices of the above departments and Crown Corporations.

For the purposes of this review, privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information.

Executive Summary (continued)

In order to provide the Government with an assessment of how privacy should be incorporated into the existing frameworks:

1. We considered *The Freedom of Information and Protection of Privacy Act (The FOI Act)* and any other relevant legislation that the departments or Crown Corporations identified to us, as this is the current legislative framework that applies to the Government of Saskatchewan;
2. We considered current practices in the public sector in Canada when developing our assessment of how the Government of Saskatchewan is addressing the rapidly changing privacy landscape, and, finally;
3. We assessed each department and Crown Corporation and the Government as a whole by developing a privacy practices questionnaire based upon the ten Canadian Standards Association's (CSA) privacy principles. We asked each department or Crown Corporation to complete the questionnaire. We held opening meetings with all departments and Crown Corporations and conducted follow-up meetings to clarify processes. We reviewed these responses, incorporated our comments and provided recommendations for each department or Crown Corporation (see Appendix A).

Each department and Crown Corporation reviewed described the legislation that they are governed by, including *The FOI Act* and described the various means that they have in place to protect personal information (including compliance with *The FOI Act*).

In a high level review of current practices in the public sector in Canada, Saskatchewan stands in much the same position as other Canadian jurisdictions. No jurisdictions have so far incorporated the CSA into their public sector legislation but are, nonetheless, reviewing their privacy practices and finding ways to use the CSA and other 'like' codes in developing government policy surrounding the protection of private information.

As part of our review we also compared the privacy processes of the 17 departments and Crown Corporations to the CSA guidelines. It is important to note that the Government must balance the privacy needs of the individual (which are illustrated through the CSA principles) against current legislative requirements and the needs of Government to fulfill mandates. In the majority of cases, informal processes exist which support the CSA guidelines. We did identify potential next steps that the Government may want to consider as the privacy concerns of citizens continue to evolve (See Recommendations Section for details).

Executive Summary (continued)

The departments and Crown Corporations with whom we met demonstrated that they treated the issue of personal information management as a serious matter, and all indicated a desire to learn how methodologies could be improved. The Government has also expressed a commitment to focus resources and attention on areas that can be strengthened and to assess how current privacy initiatives in the world may be incorporated.

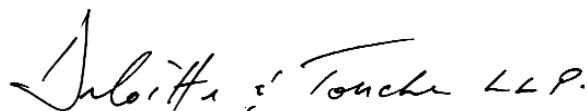
CONCLUSION

As a result of our high level review, our findings indicate that with respect to the 17 departments and Crown Corporations reviewed, on balance, the Government of Saskatchewan is managing the personal information that it is required to collect, in a fair and reasonable manner to fulfill not only its various mandates but also the policy requirements of the *FOI* legislation.

As with other public sector jurisdictions in Canada, there are, however, areas for improvement when compared to quickly evolving privacy practices and to the CSA guidelines (See Recommendations Section for details).

We would like to thank all of the departments and Crown Corporations for their attention and cooperation in this review.

... on balance, the Government of Saskatchewan is managing the personal information that it is required to collect, in a fair and reasonable manner...



DELOITTE & TOUCHE LLP

Regina, Canada
February 12, 2003

Potential Next Steps

As identified above, Saskatchewan is not alone in its review of current practices and its interest in determining next steps. Although we have used the Canadian Standards Association Privacy Principles to provide a possible template for the future, there are other privacy frameworks that the Government may want to explore (such as fair information practices).

Fair Information Practices are a set of policies, principles and procedures designed to ensure the fair, lawful and ethical collection, use and disclosure of personal information, which respect the rights of the individual.

In Canada fair information practices are encompassed in the CSA Model Code appended to the Federal Personal Information Protection and Electronic Documents Act. They are: Accountability; Identifying Purpose; Consent; Limiting Collection; Limiting Use, Disclosure and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance.

Overarching Privacy Policies

Beyond compliance with *The FOI Act*, there currently is not an overarching Privacy Framework currently in place in the government as a whole or at the departments and Crown Corporations that we reviewed.

There is a wide spectrum of privacy needs within the organizations reviewed. Several departments and Crown Corporations have very little personal information beyond having access to CPIC (Canadian Police Information Centre) terminals. Several other departments and Crown Corporations maintain a great deal of very sensitive personal information in a number of formats ranging from hard copy documents to complex computer databases.

As a result, some organizations have not focused resources on privacy management while others have spent a number of years developing processes to protect personal information.

Accountability

Although none of the departments and Crown Corporations has a designated Privacy Officer, the executive in charge or the *FOI* Access Officer is often informally filling this role. Several of the organizations outsource processing to third parties. The contracts that bind these third parties are not reviewed centrally to ensure that privacy protection clauses are standard across all contracts.

Potential Next Steps (continued)

Consent

In the majority of cases, departments and Crown Corporations use written but implied consent as part of the application process to access the programs that support their mandates. Implied consent does not inform the individual as to how their information will be used, maintained, disclosed and retained. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used, retained or disclosed. It must be “informed consent” as required by the CSA code.

Data Classification

Once information has been defined as personal information there are no classification schemes in place, which identify the type of data being stored. Data can vary in sensitivity depending upon the context of its collection – e.g. name/address may not be considered particularly sensitive with respect to land registry (a public registry) or the telephone directory and yet be considered highly sensitive with respect to a Sexually Transmitted Disease database. This must be taken into account when defining how to protect the data collected by a department or Crown Corporation.

Use, Disclosure and Retention

All departments and Crown Corporations identified application forms or verbal communications as the ways in which they inform the public as to how their personal information will be used. Very few departments and Crown Corporations explicitly inform individuals as to how their information will be shared, retained or destroyed. Often sharing is covered in legislation, Memorandums of Understanding (MOU) or Data Sharing Agreements (DSA). It may be argued that the legislation can be obtained by the public, but the MOUs or DSAs may not be readily available to the public.

The majority of departments and Crown Corporations identified the Saskatchewan Administrative Records System (SARS) and Operating Records System (ORS) as their guides to the retention and destruction of personal information.

Potential Next Steps (continued)

Safeguards

Although there were not consistent policies across the departments and Crown Corporations reviewed, many departments and Crown Corporations have policies and procedures that support privacy principles such as acceptable use policies, confidentiality agreements and information technology security policies. We have provided comments in Appendix A for each department or Crown Corporation regarding further action steps in this area.

There is no consistent application of confidentiality policies across the organizations and, as with other public sector jurisdictions, few organizations ask employees to sign off on any policies including confidentiality policies.

The government has not defined minimal physical, electronic, organizational, monitoring and enforcement criteria specifically designed for the protection and safeguarding of personal information.

Our engagement revealed that progress has been slow in most departments and Crown Corporations in response to the Provincial Auditor's recommendations on IT security in his fall 1999 report and the work of the Information Technology Office (ITO) on IT security. Many organizations identify this as still a work in progress. Since the beginning of this report the Provincial Auditor has released his fall 2002 report which has confirmed this.

Regular Reviews

Few departments and Crown Corporations identified regular reviews of how they are complying with *The FOI Act* or the protection of personal information policies, procedures and safeguards as part of their processes of attempting to ensure compliance with current processes.

Recommendations

“...Addressing privacy successfully requires more than creating great policies and processes.

An organization, as a whole, needs to understand their importance and underlying rationale, and be fully enlisted in creating and implementing them.

It needs to view privacy as necessary to assuring the ongoing viability of its business, supported by appropriate training and educational practices.

Those measures are essential to a comprehensive privacy program, since many of the potential areas for failure occur at operational levels far removed from the day-to-day scrutiny of senior managers.

Informed employees are able to spot problems readily, before they become major ones, and they are in a position to enforce the necessary policies and practices with parties outside the organization”.

Robert Merold

The Necessary Elements of Self-regulatory Privacy Regimes ...

Education needs to be throughout the organization, not just the role.

1. **Overarching Privacy Framework** - The Government of Saskatchewan should develop an overarching privacy framework (Privacy Framework) including supporting policies for all of the government departments and Crown Corporations that we examined. This Privacy Framework should recognize the need to balance privacy rights of the individual with respect to their personal information and the legitimate needs of the departments and Crown Corporations in fulfilling their public interest mandate.
2. **FOI Act** - The Government should instruct all departments and Crown Corporations to implement formal re-enforcement sessions to ensure that all employees understand their responsibilities under *The Freedom of Information and Protection of Privacy Act (The FOI Act)*. As well, once a Privacy Framework has been put in place, regular awareness should be required for employees with respect to the handling of personal information.
3. **Accountability** - The Government should establish accountability for privacy for the government as a whole and within each department and Crown Corporation.
4. **Consent** - The Government should evaluate the effectiveness of using implied consent (i.e. in some cases the assumption is made that in completing an application form, the public is often considered to have provided implied consent to the use of their personal information). From a CSA point of view, to make the consent meaningful, the purposes should be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed. It is important to note that evaluation will take into account the guidance already provided in *The FOI Act*.
5. **Data Classification** - The Government should develop a data classification scheme to identify the sensitivity of personal information. Given the rapid expansion of government data banks since the time *The FOI Act* was first enacted in Saskatchewan, there is growing need for the Government to provide for the effective safeguarding of personal information in such data banks.
6. **Limiting Use, Disclosure & Retention** – Departments and Crown Corporations should implement operational procedures with respect to use, disclosure (sharing), retention and destruction of personal information that are consistent with the government-wide Privacy Framework.

Recommendations (continued)

7. **Safeguards** - Those departments and Crown Corporations that do not have formal policies supporting the protection of personal information such as acceptable use, confidentiality or information security policies, should develop specific privacy policies, practices and procedures in accordance with the government-wide Privacy Framework.
8. **Contracts** – As the Government outsources a great deal of information processing, contracts should be reviewed centrally to ensure that privacy and the protection of information clauses are standard across all contracts. In the development of contracts with outside parties, the Government should ensure that protection of personal information clauses are built into contracts. The Government should review the audit reports provided by the outsourcers (called Section 5900 reports) to ensure that the controls identified do support the protection of personal information. Where the Government provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Government's personal information (privacy) requirements.
9. **Provincial Auditor's Recommendations and ITO Security Initiatives** - The Government departments and Crown Corporations should implement the Information Technology (IT) recommendations of the Provincial Auditor in the Fall 1999 and Fall 2002 reports to provide enhanced safeguards to personal information. As well, the Information Technology Office should continue to support the implementation of security measures within Executive Government.
10. **Regular Reviews** - The Government should implement regular reviews to ensure compliance with *FOI* and any future Privacy Framework applicable to that department or Crown Corporation, including any other privacy practices or procedures relating to that organization. This should include regular of the safeguards in place to protect personal information (such as technology reviews).
11. **Signoffs** - The Government should consider the use of annual sign offs by employees of privacy policy understanding. While we do not find that annual sign off of policies is common practice in other public sector jurisdictions, we recommend that the government move towards this as it does assist with understanding and accountability.

Recommendations (continued)

We have provided additional recommendations for each department or Crown Corporation but the Privacy Framework that is put in place will drive many of these recommendations. For example, once the overall Privacy Framework has been developed, the Government, and/or each department or Crown Corporation needs to determine how to communicate these changes to the public or to individuals who access their services. The Framework itself will drive additional processes that the Government will want to implement.

Objectives

In accordance with our Terms of Reference, we conducted the following high-level procedures in the completion of this engagement:

1. Evaluated the treatment of privacy against the Canadian Standards Association (CSA) privacy principles set out in the Model Code For The Protection of Personal Information, CAN/CSA-Q830-96 and *The Freedom of Information and Protection of Privacy Act* within the Government of Saskatchewan's day-to-day operations by:
 - Developing an understanding of the legislative and policy framework for privacy that currently exists with respect to each of the Government departments and Crown Corporations; and,
 - Evaluating the administrative processes that support privacy operationally, including an assessment of each Government department or Crown Corporation's internal administrative processes and procedures that manage the use of private information for the purpose for which it was collected.
2. Provided a general assessment of the treatment of privacy including any controls in place and overall observations on alignment with appropriate contemporary privacy practices in Canada. After gaining an understanding of the policies, procedures and practices currently in place, we used the most sensitive information identified in each organization to evaluate, at a high level the practices used to:
 - Oversee personal information privacy within the department or Crown Corporation;
 - Safeguard private information;
 - Grant and remove access permissions;
 - Monitor privacy and security activities;
 - Collect, use, transmit and store private data; and,
 - Work with employees on privacy and security matters (i.e. training, orientation, Code of Conduct, etc.).
3. Considered the recommendations of the Provincial Auditor in his fall 1999 report and the work of the Information Technology Office on IT security.
4. Ensured that the review did not conflict with any investigations being conducted by the RCMP.

Limitations

We conducted our review as follows:

1. provided each organization with an overview and privacy questionnaire;
2. conducted introductory sessions with each organization;
3. reviewed documentation provided to us in response to the questionnaire; and,
4. conducted follow-up meetings with appropriate individuals.

We did not test any of the controls identified by each organization.

The Deloitte & Touche engagement consisted of a general review of personal information privacy within each of the 17 departments and Crown Corporations. Due to the fact that this work was not an audit level evaluation, it was not within the scope of the engagement nor were procedures executed to express an opinion on the effectiveness of the internal controls identified by each organization.

In this regard, we wish to emphasize that each organization is responsible for policies and procedures to prevent and detect errors or omissions, and to identify and monitor compliance affecting them, and thus prevent and detect instances of non-compliance. In addition, each organization is responsible for ensuring that compliance measures are properly recorded and for maintaining internal controls sufficient to support compliance.

Executive Council, through the Government departments and Crown Corporations, was also responsible for making available to us, upon request, all information that we required, including all of the original records and related information from the subject Government departments and Crown Corporations, and knowledgeable personnel to whom we could direct enquiries.

The following assumptions have been made:

- That the primary purpose of the study is to help ascertain the existing level of attention given to privacy within the Government of Saskatchewan by assessing the personal information management practices of selected Government departments and Crown Corporations;
- That personal information protection policies of the Government departments and Crown Corporations, as the set of tools needed to protect the privacy and integrity of personal information assets, must be adequate;
- *The Freedom of Information and Protection of Privacy Act* and other legislation governing privacy restrict the use and disclosure of personal information and allow for its use and disclosure in prescribed circumstances. This legislative framework will, therefore, form one of the basis for the project; and,

Limitations (continued)

- That the goal of achieving reasonable levels of privacy practices with respect to personal information is constantly changing and that the appropriate measure is to compare the practices of the Government departments and Crown Corporations against current practices in the Canadian public sector and by using the CSA Standards as a guide.

Employee and business information was excluded from this review. It should be noted that, in our opinion, employee information can be treated in the same manner as the personal information of citizens.

Evolving Role of Privacy in Canada

The concept of Personal Information Privacy is not new. Writers and philosophers have discussed the concept of privacy for many years. The concept of privacy has evolved over time and through cultural influences. The concept of privacy in modern society involves very individualistic ideas that are influenced by circumstances, culture, and social position. When we speak of informational privacy in today's business and political environment, we are referring to the ability of an identifiable individual to control the collection, use and disclosure of any recorded information about themselves.

Recorded information can extend beyond traditional hard copy records to include electronic information as well as audio and videotape. The proliferation of technology and the transformation of records from paper to electronic has led to increasing concerns regarding the ease of aggregation of personal data.

While these aspects of privacy have evolved, it was not until the latter half of the twentieth century that the concept of informational privacy and the rights of citizens to protect themselves from undue, unwarranted, or illegal use of their personal information, caused governments to look at enacting informational privacy legislation.

It has been recognized that the privacy of the individual must be balanced against many competing interests. From the public sector's perspective, the privacy of the individual must be balanced against laws and distribution of the various mandates that the government oversees (e.g. health, social services).

One of the first efforts to define a code of conduct, and a standard by which personal information should be gathered, stored, used, disseminated and destroyed, occurred in 1980, when the Organization for Economic Co-Operation and Development (OECD) published its guidance. Virtually all Privacy Legislation and directives find their foundation in the OECD document.

While the public sector was an early adopter of the privacy rights of individuals, many jurisdictions, including Saskatchewan embedded those rights in freedom of information legislation in the early 1990s. Additionally, many jurisdictions introduced specific health care related privacy legislation. In the decade or more since these Acts were proclaimed the global perspective on personal information privacy has evolved to a higher level.

Evolving Role of Privacy in Canada (continued)

In Canada, the Canadian Standards Association (CSA) released the *Model Code for the Protection of Personal Information* in 1996. Although voluntary, this code has been used in the majority of subsequent privacy developments in Canada. This Q830 standard became the baseline for federal private sector privacy legislation in Canada and indeed forms an integral part of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), being incorporated into the Act as Schedule 1. Affecting the private sector, the province of Quebec is the only province that has had specific privacy legislation for many years.

In April 2000 the Government of Canada passed the PIPEDA. This Act requires that all Canadian organizations carrying on private commercial activities must be compliant with the legislation by January 1, 2004. Generally, this legislation does not include provincial governments until 2004. It also includes organizations that are involved in the selling, bartering or leasing of donor, membership or other fundraising lists. However, the Act specifies that banks, broadcasting, certain inter-provincial transportation, and those that are defined as being a federal work, undertakings or business, and those engaged in the sale of personal information outside of the province which has jurisdiction over its collection, be compliant by January 1, 2001. In addition, the Act requires that health care information be compliant by January 1, 2002. Provincial jurisdictions are able to create their own legislation prior to 2004.

The PIPEDA identifies 10 criteria, termed principles, which organizations must address (which were based upon the CSA privacy principles). These criteria apply to organizations, which fall under PIPEDA. To obtain compliance with these 10 principles organizations review and update their policies, systems and procedures, marketing and other customer facing material. In addition, procedures over the collection, use and disclosure of personal information are reviewed and made compliant with the Act. Further, adequate protection and safeguards are in place to ensure that the privacy policies and procedures of the organization are followed and the privacy and integrity of the information are maintained.

The 10 principles of the Q830 standard require much more rigor than may currently exist in provincial public sector legislation that focuses on the protection aspects and therefore confidentiality, and not on the collection, use and disclosure aspects required when dealing with privacy. Accordingly, as the privacy climate changes, new expectations are being created amongst individuals and how information about them is handled. These expectations will only increase as the private sector based PIPEDA is fully implemented on January 1, 2004. While it is clear that the mandate of the government may mean

Evolving Role of Privacy in Canada (continued)

that privacy is handled differently, it is not unreasonable to assume that individuals will expect no less of their government when dealing with personal information than their government expects of private sector organizations.

It should be noted that, for the purposes of this review, privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information.

The Freedom of Information and Protection of Privacy Act

The Saskatchewan *Freedom of Information and Protection of Privacy Act, 1990-91 (The FOI Act)* governs the Government of Saskatchewan regarding the privacy rights of citizens and access to personal information that the Government of Saskatchewan holds. See Appendix B for a copy of both the Act and the supporting regulations.

Personal information is defined as "... information that relates to the race, creed, religion, color, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual". It also includes:

- education;
- criminal history;
- financial transactions, financial history, tax information;
- received health care, health history;
- any identifying number associated with the individual;
- home or business address, phone number, (note that business address is excluded from PIPEDA);
- fingerprints or blood type;
- personal opinions or views (except where they are about another individual);
- correspondence sent to a government agency which is private or confidential in nature; and,
- the individual's name.

Personal information does not include:

- salary, benefits, expenses and duties of government employees;
- personal opinions or views of government employees when given in the course of employment;
- financial details for personal services contracts; and,
- licenses or permits granted by the government.

The agencies reviewed used the above definition of personal information when asked to tell us what personal information they maintain. The Act was well known at all agencies we reviewed and processes have been in place for many years.

The scope of our review did not include comparing the Act against the CSA privacy principles or current day privacy best practices.

Personal Information

The Saskatchewan Freedom of Information and Protection of Privacy Act defines personal information and the obligations of the Government of Saskatchewan with respect to personal information.

Comparison To Other Canadian Jurisdictions

Most provinces in Canada enacted Freedom of Information legislation in the early 1990s. That legislation incorporated certain privacy considerations and provided governments with guidance on the treatment of personal information collected, used and disclosed by the public sector. Since that time privacy concerns around the world have increased. The advent of the Internet and the ease with which data can be shared electronically have increased public concern regarding the protection of personal information. The response to public concern has varied around the world and privacy practices to address these concerns are evolving.

Global privacy initiatives have focused on developing a set of fair information practices. In Canada, the Canadian Standards Association (CSA) released the *Model Code for the Protection of Personal Information* in 1996. Although voluntary, this code has been used in the majority of subsequent privacy developments in Canada as the benchmark for fair information practices. These principles define the rights and responsibilities of individuals and organizations and provide individuals with certain rights concerning the collection, use and disclosure of their information.

While some provinces have statutory review clauses in their Freedom of Information and Protection of Personal Information legislation, based on our limited review, to date, updates to that legislation appear to address technical issues and have not incorporated the CSA Privacy Principles. There are some provinces that have used contemporary privacy practices such as CSA or the more generic fair information practices to provide guidance when developing new programs (privacy impact assessments).

Some provinces, such as British Columbia, Alberta and Ontario have drafted private sector privacy legislation and it is anticipated that British Columbia and Alberta will proceed with their legislation prior to January 1, 2004. Draft private sector legislation in those two provinces will likely incorporate the CSA model code Privacy Principles.

While adoption of the CSA Privacy principles in Private Sector privacy legislation will likely meet the “substantially similar” requirements of the Federal Personal Information Protection and Electronic Documents Act, our limited review did not identify any provinces that were currently addressing similar changes in their public sector Freedom of Information and Privacy legislation.



Comparison To Other Canadian Jurisdictions (continued)

The Federal legislation, the PIPEDA which will govern the private sector, is based upon the CSA privacy principles. As PIPEDA is based upon the CSA privacy principles, the adoption of the CSA Privacy Principles in Provincial private sector privacy legislation may result in a change in public sentiment, particularly if public sector privacy legislation is not similarly amended to provide individuals with the same privacy rights when dealing with government as will exist when dealing with the private sector.

Canadian Standards Association Privacy Principles

Canadian Standards Association

The Canadian Standards Association (CSA) is part of a non-profit membership association, which develops codes and standards around the world. In Canada, they represent ISO. The CSA's stated goals are to enhance public safety, improve quality of life, preserve the environment and facilitate trade.

In 1996, the CSA developed the *Model Code for the Protection of Personal Information*. The code attempts to balance the information requirements between businesses and government with the privacy rights of individuals. The code was designed to be used by any organization (public or private sector) that uses or collects personal information. Much of the Freedom of Information and Protection of Personal Information legislation across the country contains elements of the 10 privacy principles incorporated into this model code even though Freedom of Information legislation often pre-dates this code (as in the case of Saskatchewan).

The Government of Saskatchewan has asked us to use the CSA Privacy Principles to evaluate the current state of the protection of personal information within the 17 identified departments and Crown Corporations.

We developed questionnaires based upon the 10 privacy principles and asked that each department or Crown Corporation complete them. The principles are:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

The following provides additional detail (as published by the CSA) for each principle, as well as an overview of the government and a summary assessment of the departments and Crown Corporations:

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 1 - ACCOUNTABILITY

An organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles:

1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

1.4

Organizations shall implement policies and practices to give effect to the principles, including:

- (a) implementing procedures to protect personal information;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) training staff and communicating to staff information about the organization's policies and practices; and
- (d) developing information to explain the organization's policies and procedures.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 1 – ACCOUNTABILITY (CONTINUED)

OVERVIEW OF THE GOVERNMENT OF SASKATCHEWAN

1.1

One agency has identified an individual responsible for the development of a formal privacy program and another has a designated individual in charge of the protection of the highly sensitive personal information that the department or Crown Corporation holds. In the other departments and Crown Corporations, none have identified designated Privacy Officers. This role is often being informally filled by the executive in charge of personal information or the Freedom of Information Access Officer. In some organizations, this responsibility is dispersed throughout the organization.

1.2

The majority of the departments and Crown Corporations would make known who is responsible for personal information management, especially for *The FOI Act* access, if requested. This information is not often requested of the departments and Crown Corporations.

1.3

Seven of the departments and Crown Corporations currently outsource some or all of the processing of information to third parties. Although review of specific contracts was outside the scope of our engagement, the departments and Crown Corporations identified that information security and confidentiality clauses were built into the contracts. There was no centralized review of contracts to ensure that privacy protection clauses existed in all contracts.

1.4

All departments and Crown Corporations discussed the procedures they have in place to protect personal information. In many cases, these procedures are informal in nature and do not specifically address the privacy principles. Some departments and Crown Corporations have policies that support, but do not specifically address, the privacy principles including acceptable use policies, confidentiality agreements and information technology security policies.

The Oath of Office was identified as an important component in instructing employees as to how to protect personal information for the government departments and Crown Corporations and obtaining their commitment. Upon original hire, employees of the government sign the Oath which states "...that I will not without due authority in that behalf disclose or make known any matter or thing which comes to my knowledge by reason of my employment." This

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 1 - ACCOUNTABILITY (CONTINUED)

oath does not specifically address privacy or the protection of personal information and we did not find any interpretation or version of the oath that draws attention to this.

Procedures to receive and respond to complaints and inquiries are incorporated into the *FOI* process at each organization. No department or Crown Corporation that we reviewed had ongoing, documented formal training or awareness programs about the organization's policies and practices. Some departments and Crown Corporations had implemented these (at least on a one time basis) during our review.

The departments and Crown Corporations did not have specific packages to provide to the general public that explains how they protect the personal information in their care but they all commented that they would make the appropriate policies and procedures available to the general public if requested.

Summary of Departments and Crown Corporations

One agency has identified an individual who is responsible for developing a formal privacy program. One department or Crown Corporation has identified individuals who are responsible for managing and ensuring compliance with the policies that have been developed to protect personal information under their control (which go beyond *The FOI Act*).

Four departments and Crown Corporations have identified individuals who are responsible for complying with *The FOI Act*.

Eleven departments and Crown Corporations have dispersed responsibility for managing the policies regarding personal information and overseeing compliance with them throughout the agency.

Canadian Standards Association Privacy Principles (continued)

Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time information is collected.

PRINCIPLE 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.

2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principle.

2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle requires an organization to collect only that information necessary for the purposes that have been identified.

2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle.

2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

2.6

This principle is linked closely to the Limiting Collection principle and the Limiting Use, Disclosure, and Retention principle.

Canadian Standards Association Privacy Principles (continued)

Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time information is collected.

PRINCIPLE 2 - IDENTIFYING PURPOSES (CONTINUED)

OVERVIEW OF THE GOVERNMENT OF SASKATCHEWAN

2.1

No department or Crown Corporation has formally documented the purposes for which personal information is collected (other than that which can be inferred from the application forms), but they identified that information was collected only in support of the mandates of each department or Crown Corporation.

2.2

No department or Crown Corporation identified information collected beyond what is necessary to provide the service of the specified mandates. However, there were no formal processes in place to ensure that the required uses of the information were used to effectively limit information that is collected.

2.3

Few departments and Crown Corporations explicitly identify why information is being collected to the individuals from whom it is being collected. In the majority of cases, application forms are the means by which the public provides their personal information, which does identify how the information will be used.

2.4

Departments and Crown Corporations do not often use information for a purpose that was not previously identified, unless it is for law enforcement purposes (in these cases consent is not required by law). Therefore, they did not identify re-seeking consent as a common practice. In those departments and Crown Corporations where information might be used for a different purpose, departments and Crown Corporations stipulated that they would seek consent. These processes were not formally documented.

2.5

The departments and Crown Corporations identified that they would explain to an individual how their personal information would be used if requested through the application process. There was no formal documentation of these processes.

2.6

See Principles 4 and 5 for additional comments.

Canadian Standards Association Privacy Principles (continued)

Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time information is collected.

PRINCIPLE 2 - IDENTIFYING PURPOSES (CONTINUED)

Summary of Departments and Crown Corporations

Data is not gathered unless it is for a specific mandate within each department or Crown Corporation. Individuals provide information in order to access the service of that mandate (e.g. information provided to obtain a Health Services Card to gain access to health benefits).

Sixteen departments and Crown Corporations identified the application form as the means of identifying the purposes for which they collect information. It should be noted that nine departments and Crown Corporations do not identify the purposes for which they are gathering certain information as this is governed through legislation (e.g. tax information, law enforcement, informant programs, investigations which may lead to criminal proceedings). One agency does not collect personal information, although it does act as a custodian for much of the personal information collected, used, disclosed and maintained by departments and Crown Corporations that use their services.

Where consent is obtained, that consent is usually not formally recorded in the information databases.

The majority of departments and Crown Corporations do not have formal procedures to regain consent if they decide to use personal information for a purpose not originally intended.

Few departments and Crown Corporations describe how the information will be used, retained and shared as part of the application process.

Canadian Standards Association Privacy Principles (continued)

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PRINCIPLE 3 - CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent.

3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.

3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

Canadian Standards Association Privacy Principles (continued)

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PRINCIPLE 3 - CONSENT (CONTINUED)

For example, the names and addresses of subscribers to a news magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

3.7

Individuals can give consent in many ways. For example:

- (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- (b) a check off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
- (c) consent may be given orally when information is collected over the telephone; or,
- (d) consent may be given at the time that individuals use a product or service.

Canadian Standards Association Privacy Principles (continued)

PRINCIPLE 3 - CONSENT (CONTINUED)

3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

It is very important to note that *The FOI Act* provides for Consent as well. See Appendix B Section 28 of the Act for specific details.

If the Government were to implement the CSA Principles, the legislation above would provide direction on Consent, regardless of what CSA may recommend.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

3.1

In the majority of cases, the public applies to the government to participate in government programs. Often, participation in programs is optional and application forms explain the purpose of the program and require a signature of the applicant.

The departments and Crown Corporations felt that the application forms themselves explained how the information is to be used. In the majority of cases the application forms do not specify how the information may be retained, shared or disclosed.

As per legislation, consent is not obtained when information is used for law enforcement purposes and, in some cases, health information. It should be noted that some legal processes operate outside the ambit of *The FOI Act*.

With respect to subsequent use or disclosure of information, departments and Crown Corporations follow *The FOI Act*, so for example, details of a drivers license may be released without explicit consent of the individual. As per the Act and the supporting regulations, Memoranda of Understanding are in place between departments and Crown Corporations and external parties with respect to the sharing of information. Any other requests to release personal information would, by virtue of *The FOI Act*, require consent prior to release.

Canadian Standards Association Privacy Principles (continued)

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PRINCIPLE 3 - CONSENT (CONTINUED)

3.2

By participating in the programs, the government department or Crown Corporation considers that the individuals give written, implied consent to the collection of their personal information. The signature of the applicant records the consent. However, there are few instances where consent is explicit and informed (especially when it comes to subsequent use, disclosure and retention). There is not a formal consent statement or the ability to opt out of certain information. Nor are the consequences of not providing specific information provided to the applicant.

3.3

As departments and Crown Corporations collect information to support their mandates, there may be situations where they would deny service or access to a mandate if an individual was unwilling to provide personal information to them. There are no formal policies in place that guide this at any of the departments and Crown Corporations we reviewed.

3.4

As previously identified, in most cases consent is written but implied. In cases where sensitive health data is involved, consent is informed (e.g. application for disability benefits). No organization identified a formal data classification process, which includes sensitivity as a criterion to drive consent. Those departments and Crown Corporations with a great deal of sensitive health data identified all of their information as highly sensitive.

3.5

No department or Crown Corporation explicitly informs individuals as to whom they share the data with but this can be identified through *The FOI Act*. In no cases did departments and Crown Corporations identify situations where deceit was used to gain information.

3.6

As there are no formalized data classification schemes, which define sensitivity, there has been no guidance as to when express consent is required.

Canadian Standards Association Privacy Principles (continued)

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PRINCIPLE 3 - CONSENT (CONTINUED)

3.7

In the majority of cases, consent is given through the application form, for example, to apply for benefits in any given mandate. Check off boxes have not been used on these forms, which instruct the department or Crown Corporation not to share information. As the sharing is allowed as part of *FOI* or other legislation, research should be done to determine if individuals can opt out of allowing their information to be shared. Oral consent was identified as being commonplace and consent at time of service is often through the application form. However, if oral consent is obtained, that fact is not recorded on the applicable database.

3.8

There are no formal processes in place for an individual to withdraw consent and there would be few occurrences of this as, without the personal information, often the Government would not be able to provide the service or benefit specified in the mandate.

Summary of Departments and Crown Corporations

Eleven departments and Crown Corporations use application forms to gain consent for some or all of the mandates of their departments and Crown Corporations. One agency does not directly collect personal information; therefore, no consent is obtained.

Those departments and Crown Corporations that do not gain consent are permitted to do so through legislation.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 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.

4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle.

4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.3

This principle is linked closely to the Identifying Purposes principle and the Consent principle.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

4.1

As per Section 2, 'Identifying Purposes', in the departments and Crown Corporations that we reviewed, personal information was only collected to support the mandates delivered by the departments and Crown Corporations.

No department or Crown Corporation identified a situation to us where the information collected to deliver the programs was excessive.

4.2

We did not find evidence that information was being collected by misleading individuals about what the information was being collected for.

4.3

See additional comments in Principle 2 'Identifying Purposes' and Principle 3 'Consent'.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 4 – LIMITING COLLECTION (CONTINUED)

Summary of Departments and Crown Corporations

One department or Crown Corporation identified that they may collect more information than that which they need to fulfill their mandate. One department or Crown Corporation does not collect personal information; it only stores it. All other departments and Crown Corporations identified that they collect information necessary to support their mandates only.

The Government as a whole does not create master profiles of individuals and this is rarely done within departments and Crown Corporations themselves. Five departments and Crown Corporations did identify that they combine information on individuals. When it is done, it is often done in support of applications for permits or licenses that require criminal records checks, financial history checks, etc.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 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.

5.1

Organizations using personal information for a new purpose shall document this purpose.

5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

5.3

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

5.4

This principle is closely linked to the Consent principle, the Identifying Purposes principle, and the Individual Access principle.

As identified under Principle 3 – Consent, it is very important to note that *The FOI Act* provides for Disclosure as well. See Appendix B Section 29 for specific details.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

5.1

Based upon the CSA Principle, as many departments and Crown Corporations do not explicitly (e.g. other than inference from the application form) identify the purposes for which they collect information, nor do they record consent, it is difficult for them to know when they would need to regain consent. Departments and Crown Corporations do not often use information for a purpose, which was

Canadian Standards Association Privacy Principles (continued)

PRINCIPLE 5 - LIMITING USE, DISCLOSURE AND RETENTION (CONTINUED)

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN (CONTINUED)

not previously identified unless it is for law enforcement purposes. These processes were not formally documented. It should be noted that legislation may supercede this depending upon the circumstance of the new use of the information.

5.2

The majority of departments and Crown Corporations identified *the Archives Act* as the legislative framework, which dictates the retention and destruction of records. On a day-to-day basis, the Saskatchewan Administrative Records System (SARS) and Operating Records System (ORS) provide guidance. Some departments and Crown Corporations have their own policies as well. It should be noted that these guides have not been reviewed with current privacy practices in mind.

5.3

In the 10 departments and Crown Corporations that use SARS and ORS and the one department or Crown Corporation that does not have formal policies regarding the retention and destruction of personal information, there are not policies and procedures in place to destroy, erase or make anonymous personal data. In one department or Crown Corporation, a project is underway to anonymize sensitive personal information, which is to be used for future purposes.

5.4

See Principle 2 – Identifying Purposes, Principle 3 - Consent, and Principle 9 – Individual Access for further information.

Summary of Departments and Crown Corporations

No department or Crown Corporation has policies that guide the destruction of personal information including how long information will be kept depending upon the type of personal information. As well, no department or Crown Corporation has specific procedures in place for information that is collected and not used, e.g. when an application for a license is denied, how long is the application kept beyond overall data retention guidelines.

Canadian Standards Association Privacy Principles (continued)

Accuracy

Personal Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

PRINCIPLE 6 - ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

6.1

In the majority of cases, the definition of accuracy has not been specifically identified. There is a wide spectrum of processes in place, which address accuracy for the purposes of the particular mandate. For those programs that are annual in nature (e.g. applying for a license, permit, etc.) the information is accurate at the time of collection. In other cases, changes to personal information are requested as part of renewal or annual benefit processes. In many cases the processes used to maintain accuracy are informal within the departments and Crown Corporations.

6.2

No organization identified situations where they needlessly update personal information.

Canadian Standards Association Privacy Principles (continued)

Accuracy

Personal Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

PRINCIPLE 6 – ACCURACY (CONTINUED)

6.3

With respect to sharing information with third parties, in the majority of cases, the sharing of information is not recorded. The shared information is updated when the original recipient is informed of changes. We did not find any instances where disagreements regarding information are forwarded to the shared data recipients.

Summary of Departments and Crown Corporations

Seven departments and Crown Corporations update personal information as part of reapplication, part of annual benefit confirmations, random verifications or other ongoing means.

Three departments and Crown Corporations have nothing proactive in place to update personal information but they will do so when requested to or when changes are made known.

One department or Crown Corporation updates personal information only when a new transaction is entered into.

Three departments and Crown Corporations presume the information to be accurate and have nothing in place.

One department or Crown Corporation confirms information on each customer contact and two use normal billing and collection processes to maintain the accuracy of personal information.

When departments and Crown Corporations receive information from other departments and Crown Corporations, they do not have processes in place to ensure accuracy as they feel this falls with the originating department or Crown Corporation.

Canadian Standards Association Privacy Principles (continued)

Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

PRINCIPLE 7 - SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

7.3

The methods of protection should include:

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and,
- (c) technological measures, for example, the use of passwords and encryption.

7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

7.1

All departments and Crown Corporations identified the physical and logical security safeguards that they have in place to protect personal information. In some cases these safeguards are formalized, strong and quite restrictive (where there is highly sensitive personal information) and in other cases there are few formal processes in place.

Canadian Standards Association Privacy Principles (continued)

Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

PRINCIPLE 7 – SAFEGUARDS (CONTINUED)

The scope of our engagement included reviewing access controls at a high level and, accordingly, we cannot comment on the logical access controls that protect electronic information within applications beyond comments on the policies that have been provided to us.

7.2

As no department or Crown Corporation has defined differing levels of sensitivity, safeguards to protect personal information do not vary with respect to the collection, volume, use, distribution, and format of the information, or the method of storage. In those departments and Crown Corporations with a great deal of personal information, safeguards were described as being of a higher level.

7.3

Departments and Crown Corporations protect personal information as follows:

- (a) physical measures such as locked filing cabinets, controlled access to the building, security clearances for employees and others having access to personal information, not allowing the public access to areas where data is stored, card readers, etc;
 - All departments and Crown Corporations have policies and/or procedures in place with respect to the physical protection of data, including storage in locked filing cabinets and security clearance to the building.
 - One department or Crown Corporation has a rule that files are not to be removed from the office environment.
 - Seven departments and Crown Corporations identified additional physical security measures for CPIC terminals.
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis;
 - All departments and Crown Corporations except one (which does not directly access the data they house) identified that access to personal information by staff is on a “need-to-know” basis.
 - Eleven have IT security policies in some or all areas of the department or Crown Corporation.

Canadian Standards Association Privacy Principles (continued)

Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

PRINCIPLE 7 – SAFEGUARDS (CONTINUED)

- Seven departments and Crown Corporations that use outside contractors or outsource processing of information identified confidentiality clauses in these agreements requiring the contractor to maintain the confidentiality of the processed data. There was no centralized approach to ensuring that privacy clauses to protect personal information were included. It should be noted that the third party outsourcers used by the Government do have annual audits which provide an opinion on data centre controls including physical security (Section 5900 reports). Review of these audit reports was not identified as a common practice.
 - Five departments and Crown Corporations have codes of conduct or codes of ethics.
 - There is no specific privacy focused training that is formally documented and tracked at any department or Crown Corporation we reviewed.
- (c) technological measures, for example, the use of passwords and encryption.
- All departments and Crown Corporations identified password protection and restricted access as important technical security measures. It should be noted that passwords do not provide strong authentication to sensitive data.
 - Twelve departments and Crown Corporations identified firewalls as additional protection to external/remote access. We did not assess the parameters of the firewall tables to determine their potential effectiveness.
 - Three departments and Crown Corporations identified intrusion detection systems to protect personal information.
 - Five departments and Crown Corporations identified encryption as a means to protect information (file transfers, and secured file transfer servers, access from remote users).
 - One department or Crown Corporation identified workstations power-on passwords. It should be noted that power-on passwords for Windows 98 and below can be compromised easily.

Canadian Standards Association Privacy Principles (continued)

Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

PRINCIPLE 7 – SAFEGUARDS (CONTINUED)

- Two identified auditing features and logs to also protect information. We did not review the monitoring activities performed on the logs nor assessed the rigor with which potential problems are identified and followed up.
- One department or Crown Corporation also makes use of Public Key Infrastructure (PKI) and Virtual Private Network technology to encrypt transmissions of data.

7.4

Two departments and Crown Corporations have specific confidentiality policies for their employees. All identified various formal and informal means with which they remind staff about the confidentiality of personal information. This is accomplished through *FOI* and additional processes.

One Crown Corporation has specific confidentiality policies for employees, two departments and Crown Corporations have identified the development of confidentiality policies as important initiatives and one department or Crown Corporation has had employees resign their Code of Ethics, which contains a confidentiality clause.

Contractors and other third parties with whom personal information is shared are required to sign confidentiality agreements. It should be noted that confidentiality is only one aspect of privacy.

7.5

As identified in Principle 5 – Limiting Use, Disclosure and Retention, the majority of departments and Crown Corporations identified *the Archives Act* as the legislative framework, which dictates the retention and destruction of records. On a day-to-day basis, the Saskatchewan Administrative Records System (SARS) and Operating Records System (ORS) provide guidance. Some departments and Crown Corporations have their own policies as well. It should be noted that these guides have not been reviewed with current privacy practices in mind.

Canadian Standards Association Privacy Principles (continued)

Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

PRINCIPLE 8 - OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

8.2

The information made available shall include:

- (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and,
- (e) what personal information is made available to related organizations (e.g., subsidiaries).

8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

8.1

Five departments and Crown Corporations will share their policies and procedures if requested as part of the *FOI* process.

Two departments and Crown Corporations have other processes in place that allow them to share their policies and procedures.

Canadian Standards Association Privacy Principles (continued)

Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

PRINCIPLE 8 – OPENNESS (CONTINUED)

Nine departments and Crown Corporations have nothing formal in place with respect to sharing policies over personal information but would share if requested.

This is not applicable to one department or Crown Corporation as it only houses personal information and the data owners would make this decision.

8.2

Departments and Crown Corporations would use *FOI* to guide this process and not CSA privacy principles, thus, the requirements of Section 8.2 of the CSA privacy principles is not currently being fully addressed in any department or Crown Corporation.

8.3

Thus far, departments and Crown Corporations have not chosen proactive communication strategies; therefore, the requirement of Section 8.3 of the CSA privacy principles is not being fully addressed in any department or Crown Corporation.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 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.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 9 – INDIVIDUAL ACCESS (CONTINUED)

9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

9.1 & 9.2

All departments and Crown Corporations would provide for individual access if requested unless the information relates to criminal investigations or cannot be released for other legislative reasons. There are no policies or guidelines over the information that the individual must provide when seeking to obtain information about them to ensure all relevant information is obtained.

9.3

The majority of departments and Crown Corporations do not keep a record of third parties to which it has disclosed personal information about an individual unless it has been accessed through an *FOI* request (all of these are recorded). *The FOI Act* does provide for the sharing of information between departments and Crown Corporations. No department or Crown Corporation provides a list of third parties that it may share information with.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 9 – INDIVIDUAL ACCESS (CONTINUED)

9.4

No departments and Crown Corporations identified specific time periods in which they would respond to requests although they all follow *FOI* processes.

9.5

As identified under Principle 6 – Accuracy, all departments and Crown Corporations would change personal information if it were shown to be inaccurate, with the exception of one department or Crown Corporation that does not change data. Employees are not provided with guidance or direction on what documentation is required to demonstrate the inaccuracies or incompleteness of personal information.

9.6

This is currently handled through the *FOI* processes currently in place.

Summary of Departments and Crown Corporations

Three will allow individuals to access their own personal information.

Nine departments and Crown Corporations allow access as provided in *The FOI Act* or other relevant legislation; two of these departments and Crown Corporations identified processes used to authenticate the individual.

Three allow individuals to access their own information after their identity is verified. There are no formal policies in place on what constitutes appropriate information to enable the department or Crown Corporation to validate the identity of the requestor of the information.

One department or Crown Corporation does not allow access to personal information as it is for investigative purposes and this does not apply to one department or Crown Corporation.

Canadian Standards Association Privacy Principles (continued)

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.

PRINCIPLE 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.

10.1

The individual accountable for an organization's compliance is discussed in the Accountability section.

10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

OVERVIEW OF GOVERNMENT OF SASKATCHEWAN

10.1

Identified in Principle 1 – Accountability.

10.2, 10.3, 10.4

With respect to all of the above CSA principle recommendations:

- two have no formal processes in place but would deal with complaints if needed.
- six departments and Crown Corporations follow the guidelines provided in The FOI Act.
- one department or Crown Corporation has a formal incident reporting process and several others identified informal processes.
- three departments and Crown Corporations have formal processes to deal with complaints beyond FOI.



Canadian Standards Association Privacy Principles (continued)

PRINCIPLE 10 - CHALLENGING COMPLIANCE (CONTINUED)

- two departments and Crown Corporations have formal processes in place in some areas but not others.
- in one department or Crown Corporation, this is not applicable as they do not own the data they store.

Detailed appendices follow.

Appendices

Appendix A - Information by Department or Crown Corporation

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR)

INTRODUCTION

Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) is the department responsible for managing issues facing Saskatchewan such as site selection for intensive livestock operations, animal health, crop health, the development of the agriculture and food industries, risk management programming and coordination of rural issues to name a few. Personal information is generally collected for payment and program eligibility reasons and for taxation requirements.

SAFRR collects and uses personal information primarily with respect to three areas:

1. Individuals appointed to advisory & stakeholder committees (i.e. Board member name, SIN (payment/tax purposes), address, occupation, constituency, and organization representing).
2. Stakeholder groups – i.e. agricultural organization contact name, address, phone number, fax and email.
3. Program operations – programs such as crop insurance, Canada-Saskatchewan Assistance Program (CSAP), CCP may collect a participant's name, address, SIN and/or Sask. Health Number (for participant identification and resident eligibility).

Due to the nature of joint Federal/Provincial agreements and agricultural programs, contact and eligibility, SAFRR does collect personal information from other departments, agencies or levels of government for joint programs (i.e. CSAP). Infrequently, SAFRR shares personal information with other groups or sections within the organization. Some branches, as a result of program assignments, collect personal information for other branches. On rare occasions, SAFRR shares personal information with other provincial government departments or agencies on a case-by-case basis when requested to do so. Federal/Provincial programs administered by the province can result in information being shared with the Federal government. SAFRR infrequently receives personal information from other government departments, agencies or levels with respect to Federal/Provincial programs.

SAFRR considers personal information to be information concerning an identifiable individual that is not already in the public domain and which can be linked to an individual. With respect to personal information, SAFRR is governed by the *Freedom of Information and Protection of Privacy Act (The FOI Act)*.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

ACCOUNTABILITY

The Deputy Minister's Office (DMO) within the department, having responsibility for departmental policies as well as the actions of all Department staff, has overall responsibility. Program managers are responsible for managing personal information retained by their particular units. The Freedom of Information Access (FOIA) Officer within SAFRR is responsible for managing and ensuring compliance with legislation regarding personal information at an operational level. This position is also responsible to ensure that requests for information under *The FOI Act* are acted upon appropriately. The names of DMO senior staff and the FOIA Officer are matters of public record.

SAFRR outsources some of its processing of personal information. A service provider has been contracted to host the Revenue and Expenditure System (RES) (a pan-governmental program making payments to all vendors, including grant payments). RES is administered by the Saskatchewan Department of Finance. An outside contractor administers the data entry aspects of the crop insurance program, however, a confidentiality clause is in effect with respect to this contract.

SAFRR does not have in place specific written policies or procedures *per se* with respect to personal information. Virtually without exception SAFRR gathers personal information according to the needs of a particular program. Staff members are aware of the "Guiding Principles" (a high level document containing insufficient detail to be considered policy), which was developed by the Department. This document, combined with the Oath of Office and Orientation Manual for new staff members are the primary reference materials used by staff when determining the appropriate amount of personal information to collect and how it may be used. These materials are available to the staff through HR and are provided to all new staff. Other than upon initial hiring, training, when it does occur, is *ad hoc* and periodic.

SAFRR personnel were reminded of the need to protect personal information in a memo from the Deputy Minister on May 16, 2002. SAFRR communicates and discusses privacy protection issues with staff during initial orientation. As noted, SAFRR does not have a formal policy in place to receive and respond to complaints and inquiries, however, the FOIA Officer has been identified to handle complaints and inquiries. Monitoring of compliance with legislative requirements is not carried out overtly. Complaints are dealt with on a case-by-case basis.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

SAFRR protects personal information by securing the building after hours; ensuring offices are secured, by locking filing cabinets and through the use of firewalls to prevent unauthorized remote access. Computer files are password protected but it should be noted that passwords alone are not strong protection to very sensitive data.

IDENTIFYING PURPOSES

The determination as to the amount of personal information required by a given program is defined by the nature of the program itself and/or by legislative requirements. When programs are designed, an extensive process to determine information needs is undertaken. That process may include legal advice on the base amount of personal information needed for program purposes.

SAFRR does not classify the sensitivity of the personal information collected. Information collected that is deemed most sensitive is stored in files in locked desks, cabinets and offices. Access to electronic files is limited (but not rigorously secured) and they are protected with passwords. Program managers are responsible for managing the information. IT (Information Technology) personal information protection falls under the responsibility of the Director of Administration.

Program requirements are provided for all programs. SAFRR requests that clients supply their Health Services Card number when identification and proof of residency in Saskatchewan (required for some programs providing compensation to Saskatchewan residents). This is done in cooperation with the Department of Health through the Person Registry System. As an alternative means of identification, SAFRR requests in some cases that clients provide their Social Insurance Numbers (SIN).

Personal information is primarily used for program management purposes or to maintain contact information for client groups. The individuals who administer the programs and collect the information have been trained in the operation of the programs (but not specifically with respect to personal information and privacy). They are also provided with explanations as to why the information is needed to administer that particular program.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

CONSENT

Participation in SAFRR programs is optional. Application forms explain the purpose of the program and require a signature of the applicant. By participating in a program, SAFRR is of the view that an individual voluntarily implies consent to the collection, use and disclosure of his or her personal information.

The signature of the applicant records the consent. If the program application does not include a signature, the application is denied or returned and the personal information is not used. As well, departmental policy is in place with respect to electronically filed claims.

If the program application is signed, giving consent to use personal information, no specific monitoring is done to ensure that its use is in accordance with the consent obtained. Letters of consent are sought from the subject individual in the event of a third party request for release of personal information. SAFRR does regain consent should it become necessary to use the personal information obtained for a purpose not previously identified, however, the necessity for regaining consent is infrequent.

LIMITING COLLECTION

Program requirements define the extent of personal information required. Only that information required to administer a given program is collected. It is recognized, however, that additional information may also be collected which is collateral to the primary information required to administer a given program.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

When SAFRR obtains personal information for its programs, the information is generally not shared unless the program was designed such that sharing is a required element (i.e. Federal/Provincial programs). With respect to the retention of personal information, the Department adheres to legal requirements for auditing purposes. The Department also adheres to requirements of the Saskatchewan Archives (SARS) Schedule.

The destruction of personal information is controlled by the Saskatchewan Archives Board through SARS. The *Saskatchewan Archives Act* requires that records must be disposed of in an accountable manner. SAFRR does not collect personal information about an individual from anyone other than the individual him or herself, with the exception of certain information of public record such as land registry data.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

MAINTAINING ACCURACY

Programs or program payments are annual in nature. Applicants are required to provide accurate information when they apply, and/or to check the previously collected information when they receive a statement or re-application form.

SAFEGUARDS

Files containing personal information are stored in locked desks, cabinets and offices, all within a secured building. Paper recordings of personal information are kept in offices where access is limited – building locked during silent hours, locked wings, locked offices, front office staff direct visitors, and a commissionaire in the building. Access to electronic files is restricted and password protected. External electronic access is protected through the use of firewalls. Access to the information is limited to key staff on a “need to know” basis. Personal information is not shared with any third party unless there is consent to do so or unless SAFRR is required to do so by law.

Recently, SAFRR merged its IT department with Highways and Transportation in an effort to improve privacy, security and file protection. It is SAFRR's understanding that the Saskatchewan Information Technology Office (ITO) has implemented most of the recommendations from the Provincial Auditor's Fall 1999 and Fall 2002 reports with respect to Information Security. Several of the recommendations are currently being considered by SAFRR for implementation.

OPENNESS

Information pertaining to the collection and use of personal information with respect to a given program is provided to clients by being printed on the application forms themselves. Employees are directed to information pertaining to the collection and use of personal information on the Intranet (internal only internet site). Further, employees are informed of the need not only to protect the confidential nature of the information but the circumstances under which it may be released by means of the Guiding Principles document, the Oath of Office and the Orientation Manual (documents referred to in the Accountability section *supra*). Questions, which arise concerning access to information or appropriateness of release, are dealt with on a case-by-case basis by the FOIA officer.

Information pertaining to the collection, use and retention of personal information is usually disseminated to the public orally or as printed on application forms for the various SAFRR programs. It is not yet available via the Internet.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

PROVIDING ACCESS

If an applicant requests access to his or her own information, it is made available with proof of identity. No personal information is routinely released to the public at large. Personal information is collected on a program-by-program basis, therefore, no one individual handles all inquiries concerning access to that information. No centralized recording of access requests takes place.

Those trained in programs handle inquiries/collect information with respect to that particular program function. However, specific information pertaining to an access request may be obtained from the SAFRR FOIA Officer. SAFRR feels confident that all personal information retained by the department can be identified if necessary.

If the authority to release personal information is unclear, the department has access to legal services to obtain an opinion. If information is released through the centralized *FOI* function, SAFRR records the nature of the *FOI* request. SAFRR ensures that the authority to release information is provided for under the “consent” and “identifying purpose” sections of *The FOI Act*. The individual who receives the information is not contractually bound through formal agreements. Once personal information is released through an access request, the individual who receives it is not required to enter into a contract with SAFRR in which he or she agrees not to disseminate that information further. It should be noted that personal information released is typically of a program nature, is very individualized and is generally only provided to the individual him/herself.

SAFRR updates or deletes any information where it is shown to be inaccurate, incomplete or out of date. To confirm the amended information, applicants are generally contacted by letter or directly by telephone in the course of program administration to confirm amended information. Generally, SAFRR obtains consent when information is updated.

CHALLENGING COMPLIANCE

SAFRR does not have a formal policy in place to deal with complaints about its personal information management practices or policies. Complaints are dealt with on a case-by-case basis; however, SAFRR has not received any complaints regarding personal information management practices or policies in the past twelve months. SAFRR has not experienced any breaches of legislative requirements pertaining to the handling of personal information over the past 24 months.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

RECOMMENDATIONS

1. SAFRR should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. SAFRR should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. SAFRR should establish formal accountability for privacy within the department.
4. In the development of contracts with outside parties, SAFRR should ensure that protection of personal information clauses are built into contracts. SAFRR should ensure that this is consistent with the direction of the Government as a whole. Where SAFRR provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by SAFRR's personal information (privacy) requirements.
5. SAFRR should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. SAFRR should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed.
7. SAFRR should continue to implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
8. SAFRR should ensure that regular reviews are implemented to ensure compliance with *FOI* principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
9. SAFRR should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the department. This policy needs to balance the requirements identified in SARS with privacy considerations.

1. Saskatchewan Agriculture, Food and Rural Revitalization (SAFRR) (continued)

10. SAFRR should implement a system to record initial inquiries; the specific response and time elapsed. This should also include a record of what information was disclosed, shared, etc, in order to inform an individual of the specific information about them that has been disclosed. This should include formal procedures to be followed to authenticate individuals when information is being requested, including techniques for in-person, written, electronic, IVR and call center requests.
11. Forms and other SAFRR documents should contain specific information regarding the protection of personal information, including consent.
12. SAFRR should address electronically submitted documents and requests. We suggest an initial discussion take place between SAFRR and the ITO to discuss electronic means to accept such forms while meeting the needs of SAFRR to positively identify the individual making the submission.
13. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

2. Corrections and Public Safety

INTRODUCTION

Corrections and Public Safety (CPS) is comprised of a number of Branches, including Licensing and Inspection, Young Offenders, Protection and Emergency Services and Adult Corrections.

All Branches, to a greater or lesser degree, collect private information. Many share such information either internally within CPS or externally with other Departments of the Government of Saskatchewan. More often, however, the information is used in the creation of reports filed with the courts for pre-sentencing or sentence oversight or other bodies such as Social Services. Personal information may be made available to adjustors with respect to claims made for disaster recovery. In addition, personal information may be used in the preparation of briefing notes for the Minister pertaining to specific issues.

In addition to provincially held private information, a number of CPS Branches are allowed access to the Canadian Police Information Centre (CPIC), a repository of criminal information maintained and managed by the Royal Canadian Mounted Police (RCMP). It is noted that CPIC is governed by its own policies and procedures and is not subject to this report.

Information is identified as personal by reference to legislative authorities, including the *Freedom of Information and Protection of Privacy Act (The FOI Act)*. Other legislation governing CPS includes the *Young Offenders Act*, *Archives Act (Saskatchewan)*, *Education Act*, *Fire Prevention Act*, *Criminal Code of Canada*, *Correctional Services Act*, *Prisons and Reformatories Act (Canada)*, and the *Corrections and Conditional Release Act (Canada)*.

ACCOUNTABILITY

The Deputy Minister has overall accountability for development, policy management and compliance. All Branch Executive Directors are responsible for managing and overseeing compliance with the principles of protection of personal information.

Within Young Offenders, individual caseworkers are directly responsible for collecting, recording and utilizing personal information pertaining to clients. Supervisors are held accountable for the manner in which employees discharge their overall duties. Facility directors and regional managers, as per legislative authorities and policy guidelines, oversee the manner in which certain requests for personal information may be managed within their part of the organization.

2. Corrections and Public Safety (continued)

Overarching these responsibilities is the *Young Offenders Act* (Canada), which governs, among other things, the purposes for which information may be retained and shared and the persons or agencies empowered to secure, retain, provide and destroy personal information. Similarly, a regime of legislative/regulatory responsibility applies at Adult Corrections.

Some processing of personal information is outsourced within CPS. In many cases, programs to offenders are delivered by third party contractors, requiring that these third parties collect and deliver personal information to the Department. No specific wording appears to be routinely contained in contracting documents. However, CPS advises that Young Offenders' third party contractors are advised the information collected is subject to provisions of the *Young Offenders Act* (Canada). It is unclear whether the provisions of *The FOI Act* are imposed as well. Within Adult Corrections, binding third party contractual agreements are reviewed and approved by Saskatchewan Justice. Third party service agreements with community-based organizations include confidentiality guidelines.

Written policies, drafted by Saskatchewan Justice, are available with respect to the collection, retention, use and storage of personal information. Policy pertaining to non-personal information, such as general media enquiries, access to facility documentation, and numerous other issues is also in effect. Although these non-personal policies are not germane to the current review, they are mentioned to demonstrate the extent of Departmental policy.

Employees participate in awareness sessions during their office and job orientation sessions when hired. No regular training is in place, however, reminders are periodically disseminated throughout CPS. An oath of office in which employees pledge not to disclose any information obtained by them during the course of their employment is also signed upon hiring. No annual sign-off on privacy policy is in place. Employees having access to CPIC undergo an enhanced reliability check by the RCMP, however, no other employees are subject to such review.

Compliance is monitored through supervisory diligence and the application of policy and procedures. Security is discussed periodically at staff meetings.

IDENTIFYING PURPOSES

CPS indicates that only information necessary to carry out its functions is collected. No formal classification process exists within CPS. Highly sensitive information, the compromise of which might be expected to jeopardize safety or security, is identified and handled accordingly.

2. Corrections and Public Safety (continued)

Within many Branches, all client and case information is treated as sensitive and confidential. No formal process or policy exists to assist employees in determining the appropriate level of sensitivity and protection to be afforded to a given piece of personal information.

Personal information deemed to be most sensitive is maintained in locked filing cabinets when in paper format. Electronic records are logged as confidential and password access is restricted to the caseworker involved as well as a specified administrative support person (data input), as necessary. The case supervisor has access to both paper and electronic versions of a record.

Personal profile information is created to a limited degree, primarily within Young Offenders and Adult Corrections Branches. Individuals from whom information is collected are informed, often orally, as to the reason for the collection of the information.

CONSENT

Consent is obtained as and when necessary. Consent is implied in circumstances such as an application for Disaster Recovery funds or a license application. Some authority exists to collect personal information pursuant to the *Young Offenders Act* and other pieces of legislation. It is important to note that there are many situations where legislation overrides the rights of the individual and consent is not required to be obtained.

Memoranda of Understanding are in place between CPS and a number of other Departments with respect to the sharing of information. All sharing is accomplished within existing legislative frameworks. Employees are made aware that any unlawful sharing of personal information may result in criminal prosecution and or Departmental disciplinary action.

No specific regime is in place to monitor sharing.

In the event personal information collected is to be used for a purpose not otherwise specified, no re-gaining of consent is sought if the additional purpose is deemed to fall with consistent use or another provision that does not require the obtaining of additional consent. In some cases, verbal consent is sought. Such consent may or may not be noted in writing, depending on the circumstances.

2. Corrections and Public Safety (continued)

LIMITING COLLECTION

Application forms contain minimum statutory requirements for the collection of personal information. At times, staff is directed by court order to disclose or use personal information in a manner not previously contemplated. Court Report formats are provided to all affected staff. Policies and guidelines direct the process of assessment, case management and sentence management.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

CPS is confident that staff members are cognizant of the requirements of the oath of office to protect confidentiality and that requests for disclosure of personal information are handled through *ad hoc* channels, which have developed internal to CPS. In some Branches (e.g. Young Offenders) a Release of Information form is used to specify which information may be disclosed to whom and for what purposes. Staff orientation developed for supervisors to complete with new employees includes information on the legislative requirements of confidentiality and sharing of personal information.

Personal information collected by Adult Corrections staff is linked directly to case management activities performed by staff. Adult Corrections supervisory staff performs informal and formal audits periodically.

CPS has in place policies with respect to the retention of personal information. *The Archives Act* (Saskatchewan) and the Saskatchewan Administrative Records System (SARS) govern the retention and destruction of documents. However, Branches must also comply with other legislative requirements. For example, Young Offenders is also governed by terms of the *Young Offenders Act* (Canada). Electronic records stored in the Young Offenders Automated Client Index are never purged. Within Adult Corrections, a number as opposed to a name identifies clients.

MAINTAINING ACCURACY

CPS relies on individuals whose personal information has been collected to advise of changes to data. In many cases, personal information is verified with clients and/or professional staff when possible. Information shared pursuant to agreements is qualified as to its source. Access to Automated Client Index files is restricted to a limited number of employees who receive training in its use.

With respect to Adult Corrections, much of the personal information is static and accurate. Most adult personal data is self-reported and not verified.

2. Corrections and Public Safety (continued)

SAFEGUARDS

Disposal policies are in place with respect to personal information collected. Policies are also in place with respect to the physical security to be accorded to data, including storage in locked filing cabinets. Files are not to be removed from the office environment. No specific policies are in place with respect to identifying the nature and sensitivity of information held to assist employees in determining the appropriate level of security to be accorded.

Electronic information is password protected with restricted access. Electronic data is stored within a given Branch with access available only to authorized Branch staff. Corrections has in place firewalls to prevent unauthorized access to its information from the Internet. Logs are monitored for intrusion attempts. Remote access for authorized users is accomplished through an encrypted VPN tunnel, with Public Key Infrastructure (PKI) Certificates used to establish secure connections. Dial-in access is configured for dial-back, which controls the locations from which dial-in is available.

Staff are made aware on hiring of their obligation to protect the security of personal information, however, no annual sign-off of security awareness takes place. Security screenings are not in place for specified employees having access to sensitive material (other than those subject to CPIC scrutiny). Ongoing and periodic training in security issues takes place through briefings carried out by the FOI coordinator.

Within Young Offenders, Information Technology (IT) Policies are in place describing the restrictions on staff use of departmental systems and which specifically prohibit using them for personal gain. As noted, access to the Automated Client Index is restricted to staff who require specific information. Health information is restricted to a very small number of staff, on a need-to-know basis. Files deemed sensitive receive Restricted Access status, allowing only the caseworker, the supervisor and to the extent necessary, the administrative assistant who inputs data, access.

Similar policies are in place within Adult Corrections, including formal and informal audits of access.

IT policies are in place to restrict and define access and use to be made of electronic information.

2. Corrections and Public Safety (continued)

Third party service agreements with community-based organizations include confidentiality guidelines. ITO government wide policies are applicable within CPS, including External Subscriber Agreement Documentation. The Deputy Minister of CPS periodically reviews IT policies.

IT staff as well as the Provincial Comptroller examine new business processes within the Branch for compliance with confidentiality requirements. All proposed systems must meet IT policy standards for security. All systems are subject to an annual review by the Provincial Auditor.

Supervisors are generally experienced employees who have the benefit of years of supervisory experience. No specific regime is in place to require ongoing training with respect to privacy or security issues, however, individuals who collect personal information are required to review policy manuals and attend periodic staff meetings with respect to these issues.

Many of the recommendations contained in the Fall 1999 and Fall 2002 reports on Information Security tabled by the Provincial Auditor have been implemented while others have been considered or are in the planning stage.

OPENNESS

Policies and procedures are made available to the general public as requested. Requests pursuant to *The FOI Act* are handled as per legislative requirements.

PROVIDING ACCESS

Individuals are provided access to their own personal information. Any reference to other persons is vetted prior to sharing the requested information. Legislative and policy guidelines are followed prior to allowing access. If necessary, a hard copy of the data is vetted by legal counsel.

Media inquiries are coordinated by CPS communications personnel and are responded to by the person within the Department deemed best suited to respond. Ombudsman, Children's Advocate and *FOI* inquiries are routinely routed through the Deputy Minister.

CPS is confident that it is able to identify all personal information since such information is contained only in the client file. In the event the authority to release information is unclear, the *FOI* coordinator is consulted as well as legal counsel if necessary. Information released is always as per legislative authority.

When information is demonstrated to be inaccurate, the worker involved is responsible to update the information as part of the ongoing file management process.

2. Corrections and Public Safety (continued)

CHALLENGING COMPLIANCE

Complaints with respect to personal information management practices are dealt with through the FOI/Ombudsman process. Clients and requesters are advised of the process for challenging the release of personal information. They are informed on request of their right to appeal to the Minister. All complaints are investigated either at the local or provincial level as appropriate.

There have been few complaints registered with respect to CPS personal information management policies and practices. Within Adult Corrections, for example, only four complaints have been received in the period 1998 to 2002. Appropriate investigations have been undertaken and disciplinary action taken as warranted.

RECOMMENDATIONS

1. CPS should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. CPS should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. CPS should establish formal accountability for privacy within the department.
4. In the development of contracts with outside parties, CPS should ensure that protection of personal information clauses are built into contracts. CPS should ensure that this is consistent with the direction of the Government as a whole. Where CPS provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by CPS's personal information (privacy) requirements.
5. Given that the nature of the information held by CPS is relatively defined and static, CPS should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. CPS should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed. It is very important to note that CPS should balance this recommendation with current legislative requirements.

2. Corrections and Public Safety (continued)

7. CPS should continue to implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
8. CPS should ensure that regular reviews are implemented to ensure compliance with *FOI* principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
9. Access to the Automated Client Index should be reviewed to ensure that only those requiring access are admitted, and to ensure that only specified and appropriate individuals are able to amend records.
10. CPS should review policies with respect to the information collected, retained, handled and destroyed by the Department with privacy in mind. These policies need to balance the requirements identified in the policy with privacy considerations. Some disparity appears to exist between the requirements of certain legislation such as the *Young Offenders Act*, the *Archives Act* (Saskatchewan) and provincial policy surrounding retention and destruction of records. Use of the Automated Client Index should be reviewed and parameters set for storage and deletion of records.
11. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

3. Saskatchewan Environment

INTRODUCTION

The Department collects information in the following programs (it should be noted that not all of this information is considered personal information):

- License: Hunters, Anglers, Outfitters, Trappers, Scaling; Convention of International Trade in Endangered Species (C.I.T.I.E.S); Subsistence Fishing.
- Permits: - Timber, Grazing; Camping, Burning, Shoreland Alterations
- License Information Processing System
- Values at Risk Asset Inventory; Land Inventory Disposition System; Treaty Land Entitlement; Land Use Planning; Land Leases; Commercial Business Leases in provincial parks; Commercial Fishing (where ID and SINs are collected on behalf of the Fresh Water Fish Marketing Corporation – commercial fisherman can then apply for a subsidy).
- Environmental Assessment Review; Operator Training Database; Ozone-depleting Substances Certification Database; Registered Waste Generators/Carriers/Receivers; Registered Underground and Above Ground Storage Tank Systems and Warehouses; Drinking Water Test Results; Spills; Well Logs (WINDAT); Private Well Data (ESQUADAT).
- Critical Wildlife Habitat Protection; Firearm/Hunter Education Program; Big Game Draw; Fur Statistics; Big Game Damage Prevention; Resource Intelligence Program; Turn In Poachers (TIP) Program; Restricted Hunter Listing.
- As well the Enforcement and Compliance Branch collects more sensitive personal information with respect to prosecutions, resource use licenses, driver licenses, and Canadian Police Information Center (CPIC) records. This information is not collected on behalf of other departments, agencies or levels of government.

Within the Department, Enforcement and Compliance information is shared with law enforcement staff and programs branch staff with respect to license and permit information. As well, hunting/water samples; environmental data; land lease info; forestry contact lists for companies, land owners, and associations are shared. Big Game Draw information is shared with the Enforcement & Compliance Branch and Conservation Officers.

Personal information is shared with Federal, Provincial, and Municipal law enforcement personnel/agencies (e.g. Environment Canada, RCMP, Sask. Highways, SGI), CCRA; Sask. Social Services; Sask. Health; Environment Canada; Operator Certification Board (OCB); and the Canadian Nuclear Safety Commission (CNSC). Land lease info is shared with Saskatchewan Assessment

3. Saskatchewan Environment (continued)

Management Authority (SAMA) for tax assessment purposes; forestry contact lists for companies, landowners, and associations are shared with other government departments.

Personal information is received from Federal, Provincial, Municipal law enforcement personnel/agencies and Rural Municipalities; Environment Canada; OCB: CNSC and info re: forestry contact lists could be received from other government departments. As well, information is shared with Health through a Memorandum of Understanding with respect to Health Services Card numbers for verification purposes for the Big Game Draw.

Some Environment officials do have restricted access to the Canadian Police Information Centre (CPIC).

The Department uses *The FOI Act* to determine what is personal information as well as the *Wildlife Act* and *Wildlife Regulations*. The Department also has a Memorandum of Understanding with the RCMP re CPIC.

ACCOUNTABILITY

The “head” (Minister) is the authority responsible for access decisions and for complying with the requirements of *The FOI Act*. “Access Officers” (Assistant Deputy Minister’s and Executive Directors) are responsible for coordinating the release or denial of requested information. The “Administrative Coordinator” coordinates the process and meets reporting requirements. The Director of Enforcement and Compliance Branch manages the policies and supervises their compliance. The identity of the above individuals could be made known to the public upon request but it should be noted that this has never been requested.

The Department does not outsource any Information Technology (IT) or business processing so does not have a need to have contracts in place to protect personal information processed outside of the organization.

The Department has the following relevant written policies and procedures:

- Use of Police Information by Conservation Officers
- Intelligence Management
- Confidential Human Sources
- Computer Usage Policy
- IT Acceptable Usage Policy
- Online Transaction policy
- CommunityNet Security Policy
- Freedom of Information and Protection of Privacy Administrative Procedure Guidelines

3. Saskatchewan Environment (continued)

- Big Game Draw Policy & Procedures Manual

These policies are not publicly available as they provide staff information and guidance only. The Computer Usage Policy, IT Acceptable Usage Policy, and Freedom of Information and Protection of Privacy Administrative Procedure Guidelines are available internally on the Department's intranet site.

Many branches/ecoregions also have informal policies/processes to protect personal information.

Employees, including Parks and Fires labour service employees, received *Freedom of Information and Protection of Privacy* training in 1992. There has been no formal training since that time; new employees are trained by their supervisors or service bureau managers. Formal documentation of the training initiatives is not available. Future training is planned for the Forest Ecosystems Branch – training will be introduced under the new ISO 14001 Environmental Management System.

In the Enforcement and Compliance branch communication of the above policies to staff is done through ongoing updating and distribution of the Conservation Officer Enforcement Manual. There are no formal processes in place to communicate this to staff other than distribution of the manual. Training is provided but is not formal and no documentation is kept on when staff were trained.

To receive and respond to complaints and inquiries, the Department established 1-800 lines for resource management enforcement: TIP (Turn in poachers) line; for environmental protection, the Spills Line; and for general questions, the Inquiry Line (Communications Branch). At the Enforcement and Compliance Branch, complaints and inquiries are directed to the Freedom of Information Officer. The branch also has P-6 Intelligence Management and the Provincial Enforcement Centre procedures in place to protect personal information.

Supervisors and managers monitor compliance with existing policies and procedures.

IDENTIFYING PURPOSES

The Department identifies what personal information they maintain by looking to relevant legislation (such as *The FOI Act*). At the Enforcement and Compliance Branch, who maintain more personal information than other divisions of the Department, the identification of personal information is determined by need and seriousness of offence on a case-by-case basis.

3. Saskatchewan Environment (continued)

Informally, the Department does identify the types of information it collects and classifies it according to sensitivity (Enforcement Information is classified as the most sensitive information in the Department). Defining the appropriate level of sensitivity is done so as follows:

- Names and addresses of hunters/anglers– low sensitivity
- SIN and hospitalization # etc. - medium sensitivity
- Financial information; Business plans; environmental data – high sensitivity

The most sensitive personal information is stored in databases and filing cabinets.

The Enforcement and Compliance Branch defines the levels as follows:

- The more serious the offence, the higher the degree of sensitivity.
- Low sensitivity info – offences such as alcohol in parks.
- Higher sensitivity info – offences such as poaching or environmental infractions.

The most sensitive information concerns informants. The information at the branch is stored in electronic in-house databases, the Resource Intelligence Program. Informant's names are not sent electronically. Hard copy information is kept in a file cabinet with drawer bar locks.

Individuals have been identified as responsible for the personal information stored in the department.

The Department does create personal profiles from combining personal information from various sources. Personal profiles are created as follows: Hunters charged under the Wildlife Act can have their hunting privileges revoked; they may apply to the Director of Fish and Wildlife Branch to have hunting privileges reinstated; in order to determine if reinstatement is appropriate, the Branch will create a profile of the hunter based on information received from the Crown Solicitor, the RCMP, the Conservation Officer involved and the Enforcement & Compliance Branch.

The Enforcement and Compliance Branch also creates personal profiles for law enforcement and investigative reasons.

In some cases, the Department will inform the individuals in advance why their personal information is being collected and how it is being used. It is generally understood why the personal information is being requested, i.e. to apply for a

3. Saskatchewan Environment (continued)

license, permit or lease. When individuals question the requirement for a certain piece of personal information, the need for it is explained. Individuals interested in applying for the Big Game Draw will have advance knowledge of information to be requested by reading the Hunters' and Trappers' Guide.

The Enforcement and Compliance Branch does not inform individuals as to why their information is being used as this is used for law enforcement purposes.

When implementing a new business process, generally, the Department assesses the risks and uses appropriate safeguards/policies to ensure confidentiality of personal information. The Enforcement and Compliance Branch attempts to ensure all new business processes are adequately guarded through measures of information privacy as required by various Acts and Regulations that apply to branch activities.

To incorporate the protection of personal information when a new technology is implemented, the Department attempts to ensure all new electronic processes are adequately guarded through the use of firewalls and intrusion detection systems. Access to these systems is monitored for authorized use. Further protection is offered by limiting access, use of IDs and passwords and use of appropriate policy (e.g. Online Transaction policy, CommunityNet Security Policy). At the Enforcement and Compliance Branch, all systems are internal and are not accessible by the Internet.

Training of individuals who collect personal information is on site by the supervisor/ manager. In the Forest Ecosystems Branch, there is general training by supervisors on information to be given to clients/public and on security/retention/use of information. In the Fish & Wildlife Branch, on-the-job training is used.

CONSENT

The Department uses implied consent from individuals to collect their personal information. Information is provided by individuals on application forms or permits. Consent is implied when application forms are filled in. Currently, the forms do not tell the individual what the information will be used for, shared with, retained, etc.

The consent is recorded as it appears on the completed forms. In some cases, a signature is required (e.g. Forest Ecosystems Branch). Often, application forms are kept in the branch offices. Consent is not recorded so that it could be referenced by others. If someone feels that they have not consented, the Department does not keep a record where the individual could inquire.

3. Saskatchewan Environment (continued)

Where specific consent is obtained, the users of the personal information are informed of the consent through the supervisor or manager (often implied with no formal record kept). In the Forest Ecosystems Branch, specific consent is communicated to the users of the information by file notation, written or verbal statement.

In order to attempt to ensure that information is used in accordance with the consent obtained, the Department has limited access to data systems and information. As well, use for intended purpose and access is monitored by the supervisor or manager.

The Department uses *The FOI Act* to guide releases of personal information to third parties. This is recorded as part of the *FOI* process. It should be noted that the Compliance and Enforcement Branch does not gain consent as it obtains personal information for law enforcement purposes. For example, details of a license may be released without explicit consent of the individual. Any other requests to release personal information would, by virtue of *The FOI Act*, require consent prior to release. The Department would inform the individual and obtain consent in writing prior to release.

The Department regains consent when they want to use personal information for a purpose previously not identified. For example, they received a request from a law firm for an individual's personal information and the individual provided the Department with written permission to release the information.

LIMITING COLLECTION

The Department uses a manager's discretion to attempt to ensure that they ask for personal information they intend to use. They rely on the approved permit/application format to achieve the objectives of mandated programs. When it comes to land information, some information such as health services card/driver's license numbers are requested so that a client can be traced at a later date. The information is asked for on applications, but no mention is made that it is optional to provide the information. Some applicants choose not to provide it. At the Compliance and Enforcement Branch, the Source Coordinator or Intelligence Manager applies judgment on a case-by-case basis to ensure that they only ask for information they will need. They use two policies to guide them in this: Protocol 6 – Intelligence Management and Protocol 3 – Investigations.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

The Department follows *The FOI Act* as guidance in attempting to ensure that the personal information collected is used for that for which it is intended.

3. Saskatchewan Environment (continued)

The Enforcement and Compliance Branch limits use, disclosure, collection and retention by adhering to the following polices: Intelligence Management; Confidential Human Sources; Use of Police Information by Conservation Officers; Payment of Rewards Through SaskTip and Provincial Enforcement Centre.

The Department uses the Saskatchewan Administrative Records System (SARS) and Operating Records System (ORS) for the retention and destruction of personal information. In the case of land use, a paper copy of each cancelled disposition is retained indefinitely for the purposes of disputes and court action.

The Enforcement and Compliance Branch does not have formal policies for the retention and destruction of data. The Branch does destroy information when it is no longer in use. Inactive files, hunting license information and field check information are destroyed after 2 years while CPIC information is destroyed immediately. The Branch also collects information from sources other than the individual such as the public and other law enforcement agencies.

It should be noted that there are no policies with respect to use, disclosure, collection and retention of personal information with privacy principles in mind.

MAINTAINING ACCURACY

The Department attempts to ensure that the personal information it collects, uses and discloses is accurate in those cases where the information is valid for more than a point in time (e.g. they do not reconfirm the accuracy of information in annual licenses). In the case of Operator Training and Certification (Environmental Protection Branch), the applicant is sent a copy to verify. Information required for other license sales is confirmed by comparing to a piece of ID (e.g., driver's license). Licenses (e.g. hunters/anglers) and Big Game Draw applications are of a seasonal nature; information is accurate only on the date of application. The information is updated/changed if found to be incorrect.

The Department updates an individual's personal information if it is shown to be inaccurate. For Parks, annual financial and insurance updates are required on commercial leases. For Fish & Wildlife, Big Game Draw and Commercial Fishermen information is updated. In attempting to ensure the information is correct, the Department will confirm directly with the individual or cross-reference with other branches of department when possible. For Operator Training and Certification in the Environmental Protection Branch, the applicant is sent a copy to verify. When making amendments, consent is implied when receiving updates directly from individual.

3. Saskatchewan Environment (continued)

The Enforcement and Compliance Branch also amends information when it is shown to be inaccurate. In order to confirm the amended information, the branch follows the P-6 Intelligence Management and P15 Confidential Human Sources as guides. The branch does not gain consent from the individual before making amendments.

SAFEGUARDS

The Department uses various procedures to protect personal information from unauthorized access, disclosure, copying, use or modification. The Department stores personal information in locked filing cabinets, locks the office after hours and requires security clearance to obtain entrance to the building. The Department provides limited access to the information. Technologically, the Department uses user ID's, passwords, limited access, firewall, and an intrusion detection system to protect personal information.

The Enforcement and Compliance Branch records are under control of Enforcement Center staff 24 hrs/day. Staff are security screened to CPIC standards. Field files have drawer bar locks. Officers are security cleared and cannot have criminal records. The branch staff are CPIC cleared. Technologically, the branch uses passwords and firewalls to protect information. It should be noted that passwords do not provide strong authentication to sensitive data.

Employees, contractors, third parties and any other individuals with whom information is shared are required to sign confidentiality agreements. Third parties are provided information with the stipulation that it be used for a stated purpose only.

All employees take an Oath of Office. Confidentiality agreements exist between the branch with CPIC and SGI. As a result of the type of relationship between Saskatchewan Environment and Federal, Provincial and Municipal law enforcement personnel /agencies, the Department feels that confidentiality is understood.

In order to improve privacy and security, two Information Management Branch staff are members of the Government's Security Charter Group and are developing draft security policies.

OPENNESS

The Department communicates its policies and procedures through the Freedom of Information officer and responds to direct inquiries. The Enforcement and Compliance Branch responds via secure telephone, in person or over the radio depending on the sensitivity of the information.

3. Saskatchewan Environment (continued)

PROVIDING ACCESS

The Department allows individuals to access their personal information as provided for in *The FOI Act*. The Enforcement and Compliance Branch does not allow individuals access to their personal information as this information is protected due to law enforcement needs.

Generally speaking, release of personal information happens infrequently in this department. Typically there is only one request to release personal information each year. The only personal information that is routinely released by the Environmental Protection Branch is to an operator trainee and the Operator Certification Board (OCB), regarding operator training and certification (exam marks, status level, education) in Water Distribution, Water Treatment, Wastewater Collection, Wastewater Treatment, Small Water Systems and Small Wastewater Systems.

When releasing personal information, the Department complies with *The FOI Act*. The FOI Coordinator handles all formal *FOI* requests. If it is unclear if information should be released, the FOI Coordinator of Crown counsel advises the Department on whether to release the information or not. The Environmental Protection Branch OCB liaison handles the operator training and certification information.

The process to release information is as follows: the Department records the information that is released, the name of the recipient and the date released. For operator training and certification the Environmental Protection Branch uses a formal letter. In the case of *FOI* requests for personal information, the Department records information released, name of recipient and date released. Authentication is provided in writing unless it is from the OCB where OCB is authorized to request exam information from the Department (individuals who apply for certification to OCB sign a consent form for the Department to release their exam information to OCB).

The Department is confident that they are able to identify the personal information in their care.

The Department does not ensure that information released is provided for under the “consent” and “identifying purpose” sections. If the information is releasable under *The FOI Act*, the Department releases it.

Recipients of the information are not contractually bound to adhere with the Department privacy policies.

3. Saskatchewan Environment (continued)

CHALLENGING COMPLIANCE

The Department has a formal process in place to deal with complaints about its personal information management practices or policies as provided for in *The FOI Act*. The Enforcement and Compliance Branch follows “P-22 – Complaints about Conservation Officer conduct” to deal with these types of complaints. In the last twelve months the Department has received one complaint with respect to personal information.

RECOMMENDATIONS

1. The original training for *The FOI Act* was done over 10 years ago. The Department should provide ongoing training and formal re-enforcement on a regular basis.
2. Saskatchewan Environment should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan
3. Saskatchewan Environment should establish formal accountability for privacy within the Department.
4. As the Department has never outsourced IT processing, the Department has not developed contracts which identify how personal information is to be protected. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department’s personal information (privacy) requirements.
5. This should be done so that a policy is in place, in case the Department outsources any services where personal information is involved.
6. The Department should use the government’s data classification scheme (to be developed) to determine the sensitivity of the information under its care. Given that the nature of the information held by the Department is relatively defined and static, this may not be a time consuming exercise for the Department. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
7. The Department should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used, retained or disclosed.
8. The Department should implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.

3. Saskatchewan Environment (continued)

9. The Department should implement regular reviews to ensure compliance with FOI and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
10. The Department should develop an overarching Departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this over-arching policy, each Branch should review its current policy to ensure alignment with departmental policy.
11. The Department should develop formal procedures to be followed to authenticate individuals when information is being requested, including techniques for in-person, written, electronic, IVR and call center requests.
12. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

4. Finance

INTRODUCTION

The Department of Finance collects personal information in support of several mandates (Corporate Services, Revenue, Taxation and Intergovernmental Affairs, Saskatchewan Pension Plan, Treasury and Debt Management). The Department manages the finances of the Government of Saskatchewan.

The Department does not collect information on behalf of other organizations with the exception of the Taxation and Intergovernmental Affairs Division. This division collects CCRA income tax information, which is used for policy option analysis. When used in this way, the data is in aggregate form and the data of individual persons is not identifiable. In this Division, all non-aggregate tax data is considered personal.

Information is shared with other divisions or agencies as follows:

- The Revenue Division shares information as follows: birth dates provided to personal property registry (ISC) and Saskatchewan Health as an identifier (tax enforcement).
- The Taxation and Intergovernmental Affairs Division shares information with the Revenue Division for tax administration purposes. The Division shares CCRA income tax information with other departments on a well-justified request basis. The requesting departments would generally have to demonstrate that they have obtained permission from the individuals to have access. There is no formal policy/process that guides this.
- The Saskatchewan Pension Plan (SPP) shares address updates with Saskatchewan Health and SIN and spousal SIN information is provided to the Taxation and Intergovernmental Affairs Branch as an identifier for statistical information.
- The Treasury and Debt Management Division discloses bondholder information to legal representatives authorized to act on behalf of a bondholder and shares information related to principal and interest amounts with the Public Trustee acting as Property Guardian and with CCRA Requirement to Pay.
- The Provincial Comptroller's Division does not share the information with other government departments.

Information is received from other departments or agencies as follows:

- The Taxation and Intergovernmental Affairs Division receives CCRA income tax information from the Federal government.
- The Saskatchewan Pension Plan receives address updates from Saskatchewan Health and CCRA and death notices from Vital Statistics.

4. Finance (continued)

For the purposes of this review, the Department of Finance defines personal information as “non-business related information that identifies or is attributable to an individual”. This definition is used to determine if information is of a personal nature.

The Department, with respect to personal information, is governed by the following legislation:

- The *Freedom of Information and Protection of Privacy Act (The FOI Act)*
- *The Public Service Act 1998* – Section 22
- *The Public Service Regulations 1999* – Section 95 & 96
- *The Archives Act* and policies established by the Saskatchewan Archives Board
- Also,
 - Access to tax records is generally governed by the *Income Tax Act*.
 - The Saskatchewan Pension Plan follows the Canadian Payments Association standards for providing information in order to directly deposit pension cheques and process Pre-Authorized Contributors, which also affects the management of personal information.
 - The Provincial Comptroller’s Division is governed by the *Revenue and Financial Services Act* – Section 67 (Investigations), 70 (Secrecy), and 71 (Agreements with other governments).
 - The Treasury and Debt Management Division is governed by the requirements outlined in the Memorandum of Understanding with the Government of Canada for the exchange of information and mutual assistance.

ACCOUNTABILITY

There is no person with the overall responsibility for privacy in the Department. Each division has designated responsibility for the protection of personal information as follows:

- In the Corporate Services Division, the Executive Director is responsible for managing and ensuring compliance with policies regarding personal information. This position oversees and authorizes policy consistent with the requirements of *The FOI Act* and serves as the Department’s Access Officer.
- The following individuals oversee and authorize policy pertaining to personal information in the remaining divisions;
 - Revenue Division - Assistant Deputy Minister oversees and authorizes policy pertaining to personal information
 - Saskatchewan Pension Plan - General Manager

4. Finance (continued)

- Public Employee Benefits Agency - Executive Director
- Provincial Comptroller's Division - Provincial Comptroller
- Treasury and Debt Management Division - Assistant Deputy Minister
- In the above divisions the Directors establish and maintain policy while Managers implement and ensure compliance
- In the Taxation and Intergovernmental Affairs Branch, the Assistant Deputy Minister is accountable for managing the policies regarding information security. A Taxation Policy Analyst generally oversees the maintenance of the data.

The identity of the above individuals is made known to the public upon request with the exception of the Taxation and Intergovernmental Affairs Branch.

Taxation and Intergovernmental Affairs, the Provincial Comptroller's Division, the Saskatchewan Pension Plan, the Treasury and Debt Management Division and the Public Employee Benefits Agency outsource some processing of their data. Throughout the Department, to attempt to ensure that personal information is protected in third party care, third party contracts include information security clauses. There are no specific privacy clauses.

There are no overriding privacy policies for the Finance Department. The following policies do support the protection of personal information:

- The Saskatchewan Finance Security Policy and Procedures Manual (March 1998)
- Information Technology Acceptable Use Policy – Human Resources Manual (June 1999)
- Revenue Division Access to and Protection of Information Policy (distributed to employees July 2002)

A copy of these policies has been provided to all employees and would be made available to the public upon request. The Department has not published how the public would be able to access this information or whom to contact. To date, all awareness sessions and training on the privacy and protection of personal information has been informal. There have been recent efforts at formalizing this process as follows:

- In the Revenue division, some work units require staff to sign a declaration indicating they have read and understand the manual. The policy is being updated to require all staff to sign the declaration. The Revenue Division "Access to and Protection of Information Policy" was communicated to staff in July 2002.

4. Finance (continued)

- In the Public Employee Benefits Agency a copy of both policies is provided to all employees and is being updated to require all staff to sign the declaration. Both policies have been communicated electronically and are available on the intranet.
- SPP has a Privacy Policy (revised June 2002).

The Access Officer handles all complaints received under *The FOI Act*. Complaints respecting garnishment and third party demands are handled by the Deputy Minister's Office. No complaints have been received by the Department of Finance in this regard. The Access Officer monitors compliance with the policies and procedures through discussions with the operational units on a case-by-case basis.

IDENTIFYING PURPOSES

Each division has identified the personal information that they maintain although there is no categorization of sensitivity. Each division maintains personal information in order to administer their programs and, to date, each division has been responsible for identifying the personal information that they hold. All information obtained is given a high level of sensitivity.

In areas such as PEBA and SPP, due to the nature of pensions and benefits, little change in the information required has occurred since the inceptions of the programs.

Taxation and Intergovernmental Affairs maintains personal information as it acts as the "official" recipient of CCRA data. This data is considered highly confidential and therefore, is not categorized.

Personal information is retained in paper and electronic format for all divisions except Taxation and Intergovernmental Affairs who store only electronic data. Individuals were identified who are deemed to be responsible for this data.

The Department does not create personal profiles by combining personal information from various sources.

The Department informs individuals in advance why their personal information is being collected and how it is going to be used as follows:

- Deputy Minister's Office – acquires personal information as required to process salary garnishees and third party demands.
- Corporate Services - acquires personal information as required to respond to *FOI* requests.

4. Finance (continued)

- Revenue - In some cases, the client, whose information is being collected, signs a declaration authorizing access to the information and identifies how the information will be used (Farm Fuel Program). For tax enforcement purposes, the client is not advised that information is gathered and being used because of the nature of tax enforcement.
- PEBA - Members sign a declaration, which authorizes access to the personal information to PEBA and identifies how it will be used (pension and/or benefit programs).
- SPP - individuals provide information voluntarily when they apply for membership in the plan. Plan documentation informs the individual why the information is collected. Information is also given to members verbally.
- Provincial Comptroller - informs individuals in advance why their personal information is being collected and how it will be used. In some cases, the client provides the information and authorizes its use for the specific business purpose (Direct Deposit Requests).
- Treasury and Debt Management - informs individuals in advance why their personal information is being collected and how it will be used through a Saskatchewan Savings Bond (“SSB”) purchase application. The client signs the application.

When developing new business processes relying on the use of personal information, the sensitivity and risk associated with the information is factored into the development of the process. When implementing a new technology or system, the process is reviewed by the Provincial Comptroller’s Division to ensure compliance with Government information security policies. To date, this has not been done with privacy or fair information practices in mind.

CONSENT

Consent to collect and use personal information from individuals is gained in several different ways throughout the department. Examples follow:

- For tax enforcement purposes, consent is not gained from the client because of the nature of tax enforcement.
- Revenue - In some cases, the client provides the information and consent to collect is implied (for some programs the client must provide the personal information to qualify for the benefits). In other cases the client signs a declaration giving informed consent (Farm Fuel Program).
- PEBA - in most cases, the member provides the information and consent to collect it is implied (for some federal programs, the client must provide the personal information to qualify for benefits). In other cases, the client signs a declaration giving consent (pension). The consent is recorded either on paper copy in the Human Resources file or through the processing of program benefits.

4. Finance (continued)

- SPP - application forms are voluntarily completed by the individual authorizing consent to the collection of the information. The form does not specify the use, disclosure or destruction of the data. The consent is recorded through the creation of a member file electronically and on paper. There is no provision to record denial of use or consent for certain purposes.
- Provincial Comptroller - does not always gain consent from individuals when collecting personal information. In some cases, the client provides the information and consent is implied (Direct Deposit Requests). For operational purposes, consent is not gained from the client because of the nature of process (Demands/Requirements to Pay). When consent is obtained for Direct Deposit Requests, a direct deposit record is established in the system and a paper file is maintained to record consent. In Direct Deposit Requests, if the direct deposit record exists, consent is a given. Work unit managers monitor staff activities to attempt to ensure policy is followed and that the personal information is being used in accordance with the consent given.
- Treasury and Debt Management - does not always gain consent from individuals when collecting personal information. In the majority of cases the client provides the information and signs an SSB purchase application or bank change form giving consent to collect the information but not to use, disclose, maintain or destroy the data. When consent is obtained, a client account is established in the system and a paper file is maintained to record the consent. It is also recorded by the processing of SSB purchase/application change forms.

Users of personal information are not formally informed of the specific consent that has been obtained. In many cases, users are informed of implied, but not actual consent by the very nature of the process to use the personal information.

Work unit managers monitor staff activities to attempt to ensure policy is followed and that the information is being used in accordance with the consent. The division reviews complaints and inquiries and system and card access logs to attempt to ensure policy is followed.

When sharing personal information with third parties, consent is obtained in several different ways:

- Specific consent is required to send *FOI* information to his or her lawyer.
- In order to release individual taxation data to third parties, specific written consent is required.
- PEBA may talk to investment dealers in certain instances if the member has requested them to do so.

4. Finance (continued)

- SPP personal information is not disclosed to third parties, except in the case of marital division. Authorization for the release is covered in section 19.1 of The Saskatchewan Pension Plan Act. Other situations are dealt with by the Manager on a case-by-case basis and consent may be obtained either verbally or in writing.
- Treasury and Debt Management - when disclosing personal information to a third party, the Division does not gain consent from the individual to do so. Personal information is disclosed to bondholder's representatives at the bondholder's request.

LIMITING COLLECTION

The Revenue Division, PEBA, SPP, Provincial Comptroller's Division and Treasury and Debt Management Division attempt to ensure that they ask for only personal information they need to use through policy, training, and monitoring of staff activities. There are no formal processes in place to track the consent of individuals with respect to systems, forms design, or ad hoc surveys.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

The Department has established policies and communicated them to staff with respect to ensuring that the personal information gathered is not used for something other than the identified purpose. Access to information is restricted to only those who require it for business purposes. The activity of the employees is monitored by management in the Revenue, Provincial Comptroller's, PEBA, and Treasury and Debt Management divisions.

The Department relies on the retention guidelines established by the Saskatchewan Archives Board under *The Archives Act* (SARS Manual) with respect to the retention of personal information. It should be noted that this may be a longer period than that which the data is required from a privacy stand point. With respect to destruction of personal information, the Department follows the destruction schedules as guided by the SARS Manual. Any personal information that the organization destroys, erases or anonymizes is done so as follows: Paper files are moved off-site (marked with a destruction date) to government storage in accordance with the SARS manual; when the destruction date comes, the files are shredded.

Exceptions to the above are Treasury and Debt Management who keep records permanently and Taxation and Intergovernmental Affairs who do not have formal policies in place and maintains data for potential historical studies.

4. Finance (continued)

Electronic information contained on the network is deleted using network operating system resources. Electronic information on disc or tape is moved to a secure off-site location if archived (if not archived, the tape or disc is broken such that data is not recoverable).

The Department collects personal data about individuals from sources other than the individual in the following cases:

- Revenue - from SGI for birth dates that are used for certain tax enforcement measures and CCRA income tax information for Farm Fuel Program rebates audits (the individual provides consent).
- PEBA - from SGI for addresses and birth dates that are used for certain pension issues. The IPS/HRS system (Saskatchewan Executive Government Human Resource System) is used for both pension and benefit payments in some instances.
- SPP - collects address and birth date information from Saskatchewan Health, date of death from Vital Statistics and address information from CCRA.
- Provincial Comptroller - courts or the Maintenance Enforcement Office for third party demands and information with respect to Requirements to Pay which could originate from either the CCRA or HRDC.
- Treasury and Debt Management – from financial institutions to locate bondholders who have moved (new address and phone number) or to reimburse interest payments to bondholders who have closed/changed bank accounts or where the bondholder's financial institution has moved/amalgamated.

MAINTAINING ACCURACY

In many cases, the Department receives information from other sources who are responsible for the accuracy of the data. PEBA mails annual statements and benefit payments to members. If the information is incorrect the member may inform PEBA. At SPP, members are requested to verify personal data on their annual statements and notify the office of any changes. At the Treasury and Debt Management Division, the information is not collected until it is needed. The bondholder is contacted to confirm that the new information received is accurate and is what they want.

SAFEGUARDS

The Saskatchewan Finance Information Technology Branch, which controls information technology for the Finance divisions, has implemented safeguards for the Department. Access to paper and electronic information is restricted to those who require it for business purposes. Managers approve access in writing.

4. Finance (continued)

Sensitive hard copy information is retained in locked filing cabinets. There is restricted card access on branch doors and the server room, and motion sensors and restricted access in more vulnerable areas. There are no formal policies (and controls) on removal of files and documents from the office.

Security policies, which are available on the Finance Intranet, are in place and communicated to staff. The Divisions place a high reliance on staff integrity to protect personal information. Server logs are monitored on a regular basis to ensure there are no security breaches and a set of backup tapes is retained off-site in a secure environment. Access to information on the network is managed by network permissions and user id/passwords. All workstations have power-on passwords. It should be noted that Windows 98 and below can be compromised easily. All systems and information sit behind a firewall. At login, users must accept the Saskatchewan Government Information Technology Acceptable Usage Policy before continuing login.

There is a change management process in which new systems or technologies are reviewed and approved prior to implementation. This guides the Information Technology Branch to comply with Government and Finance information security policies. To date, a privacy component has not been built into this process. With respect to improving security, the Divisions (except the Provincial Comptroller) conduct periodic reviews of staff network permissions and access and review the information security policy.

All third party contracts entered into have confidentiality agreements. To date privacy has not been included in the contracts. At the Corporate Services Division, one of the roles of the Executive Director is to review Finance's contracts before recommending them for signing to the Deputy Minister. A significant check is made to ensure that confidentiality clauses are included in all agreements.

Currently, staff are not required to sign a confidentiality agreement. Policies regarding the review of access logs are currently being developed in the Revenue Division Access to Information Policy. As well, at the Revenue Division, an agreement for the staff to sign is currently being developed and will be implemented in the near future.

At Taxation and Intergovernmental Affairs, access to CCRA data on the mainframe is limited by CGI Information Systems and Management Consultant's ("CGI") security systems to safeguard personal information. Access to the electronic information is managed by network permissions and user id/passwords.

4. Finance (continued)

OPENNESS

The policies, procedures, contracts, etc., used by the Department to protect personal information are available to the public through *The FOI Act*. The exception to this is at Taxation and Intergovernmental Affairs, staff are advised that public requests for access are to be directed to CCRA. Requirements for accessing information are communicated to other departments of government on a per-request basis.

Internally, policies and procedures are communicated orally, in paper form, electronically via e-mail and files and through the Finance/PEBA Intranet.

PROVIDING ACCESS

The Department allows individuals to access their personal information. *The FOI Act* governs access to the information and the process to release personal information. No information is routinely released; all requests must go through *The FOI Act*. In the Revenue and Comptrollers divisions there have been no inquiries made for this information. At PEBA, information regarding disability benefits has been released in the past through *FOI*. No procedures were specified to identify how individuals are authenticated.

Regarding release of information for SPP, correspondence is mailed to the member's address as provided by the member. Verbal requests for information are only released when staff are satisfied they are releasing it to a member. There is no formal record of what information has been released or when.

The Access Officer handles all the inquiries for release of information. If the authority to release personal information is unclear, the Corporate Services Division obtains advice from Finance's solicitor with Saskatchewan Justice. When information is released, the name of the recipient and the date released is documented within each case file. If the information is to be released to anyone other than the individual himself/herself, he/she must give specific consent before the information is released.

At SPP, if the authority to release personal information is unclear, the plan obtains advice from the Area Manager, Justice and/or FOI coordinator at Finance.

At Treasury and Debt Management, if the authority to release the information is unclear, SSB program staff pursue and consult managers if they could not resolve the issue.

4. Finance (continued)

The most often released information for the Treasury and Debt Management is bondholder transaction history. The division obtains written/verbal consent from the bondholder or bondholder representative to release the information.

Requests for personal information to the Taxation and Intergovernmental Affairs Division are directed to CCRA. If access to information is required through the Division then *The FOI Act* governs the public access to the information. The process to release personal information to the public is outlined in the *Act*. No information is routinely released, as there have been no inquiries made for this information. Any data that is out of date or needs to be amended is updated from CCRA.

In confirming amended information, SPP collects the information from reliable sources and verifies and obtains consent from the member to make the amendment.

The Provincial Comptroller's Division does delete or update information when an individual's information is out-of-date. The information is collected from reliable sources and supporting documentation is required from that source before any adjustment is made. When an adjustment is made, the Division does not gain consent from the individual to make the change.

At PEBA, all information collected by the Division is deemed reliable and, therefore, no steps are taken to ensure amended information is reliable (rely on the accuracy of the source such as SGI, member, family member, power of attorney, employee). If information is found to be inaccurate, the client is contacted to confirm the information.

At Treasury and Debt Management, the Division does update personal information such as bondholder address, banking and SIN if it is out of date. To confirm the information collected is correct, the information is collected from reliable sources. If the information collected is found to be inaccurate or received from a source considered not reliable (such as Canada Post remark on returned bondholder mail), the client is contacted to confirm the information.

CHALLENGING COMPLIANCE

When dealing with complaints or inquiries about the Corporate Services Division's management of personal information policies and practices, a formal process exists. All complaints under FOI would be handled by the Access Officer. Garnishments/third party demands are handled by the Deputy Minister's Office. That said, no complaints have been received by the Corporate Service division in this regard.

4. Finance (continued)

Compliance with existing policy and procedure is monitored by work unit managers who attempt to ensure staff members are following the policies. In some divisions, review of complaints and inquiries and monthly management meetings where issues are reported are other ways the department attempts to ensure compliance with the policies.

Revenue, PEBA, SPP, Comptroller, and the Treasury and Debt Management Divisions also have formal policies in place when dealing with complaints or inquiries about the Division's management of *The FOI Act*. Complaints or inquiries of any nature are usually handled by the work unit Managers. However, the point at which the complaint is received governs the process. Complaints received at the director or minister level may be replied to at that level. Potential contentious issues are communicated to the appropriate level. Judgment, not written policy, governs this process. The Freedom of Information Commission also handles complaints regarding requests/withholding information.

At the Taxation and Intergovernmental Affairs Division, personal complaints or inquiries about taxation data are generally handled by CCRA. The Division would direct individuals to CCRA.

RECOMMENDATIONS

1. Finance should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. Finance should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. Each division should develop policies and procedures, which support the overall Finance policy.
4. Finance should establish formal accountability for privacy within the Department.
5. In the development of contracts with outside parties, Finance should ensure that protection of personal information and privacy clauses are built into contracts. This should be consistent with the direction of the Government as a whole.
6. Finance should expand the work currently being done in the Revenue division to the entire department.
7. Finance should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.

4. Finance (continued)

8. Finance should, along with the Government as a whole, evaluate the effectiveness of using implied consent in non-legislative situations (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed.
9. Finance should continue to implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
10. Finance should ensure that regular reviews are implemented to ensure compliance with *FOI* principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
11. Finance should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this overarching policy, each division should review its current policy to ensure alignment with departmental policy.
12. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
13. Finance should implement a system to record what information was disclosed, shared, etc, in order to inform an individual of the specific information about them that has been disclosed.
14. Finance should develop formal procedures to be followed to authenticate individuals when information is being requested, including techniques for in-person, written, electronic, IVR and call center requests.

5. Health

INTRODUCTION

Saskatchewan Health collects personal information in the following categories:

- Registration information (typically demographic information) collected pursuant to *The Department of Health Act* to register individuals for benefits provided through provincial programs.
- Prescription drug information collected pursuant to *The Prescription Drugs Act*.
- Physician billing information collected pursuant to *The Medical Care Insurance Act*.
- Hospital admission/discharge information collected in support of provincial planning, monitoring and support for hospital services.
- Vital statistics data pursuant to *The Vital Statistics Act*.
- Personal information in support of various programs administered by the Department such as Supplementary and Family Health Benefits, Saskatchewan Aids to Independent Living, etc.
- The FOI Directory provides additional information to the above.

In support of its mandate to ensure effective and efficient coordination and delivery of health services, including support for regional health authority delivered services, the Department will host information technology systems that contain information collected by individual health regions. Systems (such as the Mental Health Information System) are typically designed to allow only the region that provided the data with access to that data. In regard to these systems, Saskatchewan Health views itself as an information manager, rather than a data collector.

Saskatchewan Health shares information in accordance with its programs and mandates. Disclosures of personal information are limited and specific to the purpose for which the information was collected or to a consistent purpose (such as providing a health service or paying for that health service).

Other government agencies and departments rely on the Person Registry System established and maintained by Saskatchewan Health to register residents for health benefits. In accordance with *The FOI Act* (section 16 of the Regulations under *The FOI Act*) Health will disclose limited information to other government programs or activities primarily for the purpose of verifying residency and accuracy of personal information.

5. Health (continued)

The Person Registry System has been developed as a mechanism to identify citizens of Saskatchewan. With respect to the Person Registry System, individual agreements or Memorandums of Understanding (MOUs) are on file to support the sharing of information and the stipulations surrounding the release of any personal data. Limits are placed on the information provided and/or the acceptable uses of the information provided. For example, Health maintains an agreement with Department of Learning to assist in the auditing of Student Loan applications and Employment Subsidy/Training Allowance nominations for residency. Learning provides Health with a batch of Health Services Numbers (HSNs) collected from students applying for Learning benefits. Health verifies that they are valid HSNs, thus confirming residency requirements for the students. No health information is provided in the process.

Saskatchewan Health has reviewed long-standing arrangements for access to the Person Registry System information. While the agreement between Social Services and Health is dated, it does place limits and controls on what the information can be used for. Nevertheless, as a result of the review, Health and Social Services, several years ago, launched a major overhaul of the systems and controls in place to further limit access to the information to a need-to-know basis.

MOUs for access to the Provincial Health Registry exist for:

- Agriculture and Food (Conservation Cover Program, Farm Land Education Tax Rebate)
- Saskatchewan Cancer Agency (Screening Program for Breast Cancer)
- Finance (Farm Fuel Tax rebate)
- Justice (Jury Selection)
- Public Trustee (Administration of Estates)
- Post-Secondary Education (Provincial Training Allowance, Student Loan Program)
- Environment and Resource Management (Big Game Draw)
- Revenue Canada (Collection of Tax Owed to Saskatchewan)
- Canadian Blood Services (Contact Tracing)
- Saskatchewan Abilities Council (SAIL Equipment Loan)

The above list does not include special pilots or projects.

The Department receives personal information from regional health authority boards (local government) in support of its mandate to provide and administer certain health services within the province. The Department only receives

5. Health (continued)

information consistent with its mandate and in accordance with legislation. For example, Health will receive summary information from regions for hospital visits. The Department uses this information to support its role in planning, payment and delivery of services. The Department may also receive case-specific clinical information from regional health boards in response to requests from individuals for help from the Minister or Department in specific cases. In such circumstances information is provided under authority of *The FOI Act*. It is important to note that most health and personal information collected by regions for health services is not provided to the Department.

The Department may also receive information from other government departments in relation to registering individuals for provincial health benefits. For example, if a resident from another province is incarcerated in a Saskatchewan jail or penitentiary, Saskatchewan Justice will electronically register the individual for health benefits for the period of incarceration. Similarly, Social Services can nominate individuals for supplementary health benefits by providing information to Health.

Personal information is determined primarily by reference to definitions in statute. The definition in *The FOI Act* is the primary reference.

The Department is governed by the following legislation in respect of personal information:

- *The Freedom of Information and Protection of Privacy Act*
- *The Health Information Protection Act* (not yet proclaimed)
- *The Medical Care Insurance Act*
- *The Prescription Drugs Act*
- *The Department of Health Act*
- *The Saskatchewan Hospitalization Act*
- *The Public Health Act*
- *The Personal Care Homes Act*
- *The Mental Health Services Act*
- *The Housing and Special Care Homes Act*
- *The Hospital Standards Act*
- *The Home Care Act*
- *The Regional Health Services Act*
- *The Change of Name Act*
- *The Vital Statistics Act*
- *The Ambulance Act*

5. Health (continued)

In addition to the above legislation, the Department uses activity specific requirements for confidentiality beyond what is required by legislation. For example, ethical considerations for the use and or disclosure of personal information for research purposes. *The FOI Act* provides the ability to disclose personal information without consent for research purposes. Health follows criteria that are more restrictive than *the Act* in terms of what may be disclosed. The Department has established a Data Access Review Committee (DARC) to review all requests for data linkage and disclosure. DARC follows strict criteria that ensure that identifiable data is never disclosed for research purposes without consent.

ACCOUNTABILITY

The Director, Health Planning/FOI Coordinator is accountable for managing the policies regarding personal information and overseeing compliance with them. This position was created in 1997 to lead policy initiatives related to the protection of personal health information. The position is principally responsible for development of *The Health Information Protection Act* (“HIPA”), interpretation and enforcement of *FOI* within the Department, along with providing advice and direction throughout the Department and the health sector on privacy issues. The role of this position is understood throughout the Department and Managers are expected to (and do) raise any issues or questions regarding personal information with this position. Policy and Planning Branch works with all branches to ensure that practices, criteria, guidelines and policy are in compliance with good information practices, applicable legislation and Department policy.

Each Branch Head (typically an Executive Director) is responsible for policy related to their area of activity. Policy is typically developed in consultation with the Director of Health Planning. The Human Resources Branch is responsible for staffing actions which may be required if a policy is violated. The identity of the above individuals are made public when requested.

Saskatchewan Health contracts with CGI and ISM for the provision of data management services. The Department enters into legal agreements binding the service providers to confidentiality. It is worth noting that, in the ISM contract, Health was able to negotiate protection for the personal information beyond the life of the contract – which is not usually done by ISM, but recognizes the significance of confidentiality requirements for the protection of personal health information.

5. Health (continued)

The Department has the following policies with respect to personal information:

- An *Information Management Policy for Saskatchewan Health* was approved in 1995 by the Executive Management Committee. It has served as one of the starting points for several years of policy work leading to the creation of *HIPA*. For the past several years, *HIPA* has served as the principal written policy associated with personal information in the Department. In addition to other legislation, it guides all policy conversations regarding personal information.
- An *Acceptable Use and Security Policy*
- Application or branch specific written policies for personal information within that branch. For example, Health Registration and Vital Statistics has written policy for appropriate use and disclosure of information from the Person Registry System.

A Department wide review of personal information practices was initiated in 2000-2001 to ensure compliance with *HIPA*. The review was temporarily postponed pending amendments to *HIPA* which were intended for Spring 2002. Aside from the *HIPA* review, policies continue to be reviewed as required (such as when a program is changed or the information system is updated, created or modified).

Department policy is to provide all new employees with an orientation that includes:

- Taking an Oath of Office which prohibits disclosure of any kind without authorization
- Orientation to the specific requirements of each position, including reference to any relevant policies and procedures
- Individual managers are responsible to ensure that staff are aware of policies specific to their areas

In addition, the Department conducts awareness initiatives for all employees to make them aware of policies regarding appropriate use of information access and information technology. Specifically:

- June 28, 1995 – Deputy Minister circulated the *Information Policies for Saskatchewan Health* to all branch heads
- July 15, 1996 – Deputy Minister memo to all staff re use of computing resources policy
- January 4, 2000 – Deputy Minister memo to all staff re IT acceptable use and security policy

5. Health (continued)

- May 16, 2002 – Deputy Minister email to all staff re confidentiality of information (reminder)
- June 2002 – series of awareness sessions with staff in all branches
- Ongoing – intranet and orientation for new staff

Employees receive orientation upon start of employment. This includes awareness of Department wide policies as well as those specific to their area of responsibility. The latest training or awareness sessions were held in June, July and September 2002. All branches were required to participate in a presentation and discussion of department IT Acceptable Use and Privacy Policies. As part of this training, it was stated that “Saskatchewan Health” has a zero tolerance for unauthorized use or disclosure of confidential or sensitive information and, for unacceptable use of its IT resources.

The FOI Unit in Policy and Planning Branch accepts public complaints and inquiries regarding personal information. Contact information for this unit is available publicly, including on the Internet and in the government’s FOI Access Directory. Programs that deal directly with the public have established public reception areas and procedures for interacting with the public. For example, Health Registration has a public area, provides information about services, is available to answer questions related to the registration for health services, and can respond to customer concerns and complaints.

Monitoring compliance with policies and procedures is accomplished in several ways:

- Individual branch heads and program managers are responsible to ensure that staff are following established policy and procedures.
- As electronic information management systems are developed or updated, systems are reviewed to ensure compliance with HIPA and other legislation. Steps are taken to improve privacy, for example auditing systems (i.e. access logs) are added to new systems where needed.
- Individuals are reminded that they are responsible for compliance with policy and are encouraged to apply peer pressure, to modify their own behavior and report violations regarding inappropriate use.

IDENTIFYING PURPOSES

To determine what personal information the Department maintains, periodic department-wide inventories are conducted. For example, *The FOI Act Access Directory* was updated in 2000 and an inventory of all personal health information systems, in preparation for proclamation of *HIPAA* was begun in 2001.

5. Health (continued)

The general public typically considers personal health information to be among the most sensitive types of personal information. The Department considers all personal information it collects to be very sensitive and applies high levels of confidentiality and security to all the information it collects.

All personal health information is sensitive and kept confidential. Legislation may identify higher levels of sensitivity for certain information (e.g. laboratory tests such as HIV, and prescription drug information). Individual program managers, often in consultation with the Policy and Planning Branch, consider appropriate use and protection of personal information, including giving consideration to the level of sensitivity.

Sensitivity of personal health information is often specific to the individual the information is about (i.e. what is relatively minor to one person may be highly sensitive to the next). Therefore, Saskatchewan Health considers all personal health information to be sensitive.

The data collected by Drug Plan and Extended Benefits Branch (DPEBB) and the Provincial Laboratory contains some of the most sensitive information held by the Department. The following explains how this sensitive information is housed and protected.

Drug Plan

Personal health information in DPEBB includes:

- Prescription records (benefits drugs for Saskatchewan beneficiaries)
- Special coverage requests (such as requests for Exception Drug Status, Palliative Care, Plan Two, etc.)
- Special Support applications (financial assistance)
- Long-Term Care income testing
- Supplementary Health payment records (dental, optical, medical supplies, ambulance, etc.)
- Saskatchewan Aids to Independent Living (SAIL) payment records (equipment, oxygen, etc)

The prescription drug on-line system is housed at CGI, under contract with Saskatchewan Health. It should be noted that all contracts with third parties contain clauses ensuring the confidentiality of the information that they house for the Department. Claims are entered into an on-line network by pharmacies and Drug Plan staff, and are adjudicated for benefits. Historical prescription records are received monthly from CGI and stored on a Health network drive by Corporate Information Technology Branch of Saskatchewan Health (CITB).

5. Health (continued)

The claims payment systems for Supplementary Health and SAIL are maintained and housed by CITB. Similarly, the long term care admissions and income testing system is maintained and housed by CITB. Applicable network security applies in all cases. Various paper records are received (fax and mail) for processing. These include claims for prescription, supplementary health, or SAIL benefits; applications for the Special Support Program; requests for special coverage; and documents related to long-term care income-testing. Requests for special coverage are also transcribed into paper form by Drug Plan staff from a 24-hour telephone message system. All paper records are received, opened and stored in a no-public area in the branch. Archiving and storage follow Archives Act.

Provincial Laboratory

The Provincial Laboratory completes medical lab tests on specimens received directly from health regions or referred to it from regional laboratories. Over 90% of tests in the province for communicable and sexually transmitted diseases are performed at the provincial laboratory. Lab results are maintained in the Laboratory Information Management System (“LIMS”) and are only accessible by selected staff in the Provincial Laboratory to resolve technical system issues. The system is fully ID and password protected.

Physical access to the Provincial Laboratory is restricted by electronic card access, supplemented by physical security at the entrance to the building. The computer system is housed in a secure physical environment. Access is available through two levels of electronic security cards. An additional combination door lock that is only available to a very limited number of staff.

An electronic copy of the test results are downloaded from the LIMS system into a separate database for electronic distribution. This database is used for Public Health purposes and is accessible only by selected Provincial Laboratory staff and the Medical Health Officers in the province. Medical Health Officers access this data through Public Key Infrastructure (PKI) technology.

The Department maintains various databases and does combine data in a limited fashion. For example, the Person Registry System is used to support numerous program specific systems throughout the department, PRS data is combined with physician billing data for the purposes of the Medical Services Plan; PRS data is combined with prescription drug data to complete the Drug Plan database, etc. Data linkage beyond that is subject to review by the Data Access Review Committee.

5. Health (continued)

Most personal information collected by Health is collected from secondary sources and is done so as a requirement of legislation. Where the Department collects personal information from individuals it is for a specific purpose and typically in accordance with the completion of applications. For example, individuals are required to register with Saskatchewan Health to receive provincial health benefits. Individuals complete a registration form specific to that purpose and are provided with additional information as necessary. A brochure called *Its For Your Benefit* explains the benefits that are provided and is readily available to the public.

In preparation for proclamation of *HIPA*, Health has been reviewing data collection practices to ensure that individuals are informed of the purposes for collection and of anticipated use and disclosure of the information.

New business processes are reviewed by the Policy and Planning Branch to attempt to ensure they are compliant with *FOI* and consistent with *HIPA* and existing Department policies and standards. All new computer systems are subject to review by the Security Audit group of the Corporate Information and Technology Branch. One of the components of this Security Audit is to ensure that only minimum “need-to-know” access to information is given to individuals entering the system.

HIPA, which was developed by the Department, requires that individuals be informed about anticipated use and disclosure of personal information when the information is collected directly from the individual. As the Department works towards *HIPA* compliance, programs are reviewed to ensure that they meet this requirement.

Saskatchewan Health primarily collects personal information from secondary sources. There is often no ability to speak directly with the clients. In areas where personal information is currently collected directly from the public, information is made available regarding the purpose. For example, the brochure – *Its for Your Benefit* describes the benefits received as a result of registering for services.

CONSENT

As part of the DARC process to review requests for data linkage and release for research, no identifiable data is released without specific and informed consent from the individual the information is about.

5. Health (continued)

Most personal information collected by the Department is done so in accordance with the legislation and the Department feels that consent is not a requirement or an issue. For example, all residents are required to register for health benefits in accordance with *The Department of Health Act*. In preparation for *HIPA*, the Department is reviewing all information collection practices and will apply consent where needed. Policy and Planning Branch reviews individual consent issues and advises on what is required to ensure consent is valid and is consistent with *HIPA*.

The recording of consent varies from program to program; however, consent is generally recorded in accordance with legal requirements of *FOI*, *HIPA*, or legislation specific to the activity. As part of the preparation for proclamation of *HIPA*, Policy and Planning Branch advises on consent processes when new programs are created or as programs are reviewed.

If consent is required for use of personal information, then the consent is collected specific to a program or activity. Users will only use the information in accordance with the program or activity.

Branch heads and program managers are responsible for ensuring that personal information is only used in accordance with the needs of a particular program or activity, including meeting any requirements for consent. The Policy and Planning Branch provides advice and input regarding consent and appropriate use of information based on that consent.

HIPA provides rules regarding consent. As the Department prepares for *HIPA*, all consent requirements will be reviewed and made *HIPA* compliant. All programs that allow external access have logging and tracking systems. Access is only provided with a defined set of circumstances and in accordance with the law (e.g. Medical Health Officers accessing certain Lab Records). The Department is planning a new version of the Person Registry System, which will include tracking logs for all internal access as well.

Unless permitted by law, Saskatchewan Health will not disclose personal information without the consent of the individual. Even when permitted by law (e.g. conducting research), Health may have criteria, policy or guidelines that will require consent of the individual before information can be disclosed. When consent is required, the Department ensures that it is specific to the need, that a proper description of the disclosure is provided to the individual, and that the individual has the opportunity to decline to consent.

5. Health (continued)

If Saskatchewan Health wants to use or disclose personal information for a purpose that is not permitted by legislation or where consent was previously gained for a different purpose, Saskatchewan Health will seek consent. For the most part, the Department only uses personal information for purposes provided for in legislation or through its mandate (i.e. the purpose for which the information was collected). In other instances, for example, conducting research, a new consent is gained as required.

LIMITING COLLECTION

The *FOI* statute, which limits collection to information needed for existing or proposed services or activities, binds Saskatchewan Health. The Policy and Planning Branch will review proposed programs to ensure they are compliant with both *FOI* and *HIPA* (and any other relevant statute), including limiting collection to only that which is required.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

The Policy and Planning Branch is responsible for providing support, advice and development of information policy. Policy and Planning works with individual branches to review programs using personal information, and advices on appropriate use and disclosure of that information. Individual branches are responsible to ensure that information is only used for the purpose the information was collected. If a need is identified which is not consistent with the original intent, the action is reviewed with Policy and Planning to ensure it is acceptable under law and, where necessary, consent is sought.

HIPA has rules regarding use, disclosure, collection and retention of personal health information. As identified previously, all personal health information processes are being reviewed in preparation for *HIPA*.

Health complies with retention schedules approved pursuant to *The Archives Act*. Once records are eligible for destruction, the following may occur:

- Records are shredded by support staff in secure/nonpublic areas
- Records are sent off-site to the SPMC Records Centre, where destruction is arranged
- Records companies (such as Crown Store-All) are contracted to securely shred or dispose of records

With respect to retention and destruction after useful life, most personal information is collected for health purposes and has ongoing use and value. It should be noted that this may conflict with current privacy practices. Health is currently investigating methods of retaining anonymized data for long-term use not directly related to the purpose the information was collected.

5. Health (continued)

The Department collects data primarily from secondary sources. For example: In order to fulfill obligations under *The Medical Care Insurance Act* Saskatchewan Health received billing information from physicians that includes personal information about patients that have received service. Similarly, the Department collects personal information from pharmacies in regard to prescriptions in order to fulfill the requirements of *The Prescription Drugs Act*.

MAINTAINING ACCURACY

Steps taken by Saskatchewan Health to ensure the accuracy of data varies from process to process. One example of the processes used within the Department to ensure data accuracy is as follows:

- Medical Services Branch maintains possibly the largest single database of personal information held by the Department. Each year the Branch receives and processes approximately 9 million claims for payment for physician, chiropractor, optometrist and out-of-province health services. The Branch has a number of manual and automated assessment systems in place to ensure that the information submitted on these claims is accurate before payment is made and the data enters the statistical databases maintained by the Branch. Throughout the assessment process:
 - The personal information for each beneficiary for whom a claim is being submitted is verified against the Personal Health Registry for accuracy;
 - Information on the health professional submitting the claim is verified to ensure that the individual is eligible to submit a claim under the plan;
 - Service information is verified to ensure that the service being provided is eligible for payment based on the beneficiary's personal information and medical history and payment schedule assessment rules.

Once the claim is paid, the data becomes part of the patient history. The branch maintains statistical records of payment and services provided. The accuracy of these databases is verified internally and by the Provincial Auditor.

As well, the Branch undertakes ad hoc claim verification and professional review processes to ensure the integrity of the claims submitted. This includes sending 100,000 verification letters to beneficiaries to ensure that the claim submitted by the provider is accurate in all details. As well, an internal unit and the Joint

Medical Professional Review Committee ensure that billing practices of providers meet a standard of practice acceptable to the profession.

5. Health (continued)

SAFEGUARDS

The Department has a number of physical measures in place to safeguard information, including:

- A commissionaire maintains a desk at the front door and visitors are expected to register although the commissionaire does not stop people who do not register.
- Areas open to the public (e.g. Health Registration, Vital Statistics, Drug Plan and Extended Benefits) have public reception areas that separate the public from any personal information on file.
- Most personal information is maintained in computer systems that are protected by limiting availability to certain computers, user ID and password protection, as well as physical separation and protection of servers, which store data.
- Applications containing personal information are only available to those employees that need to know the information to do their jobs. Those employees use that personal information within the context of their own work. Any other use or disclosure must be brought to the attention of the manager and, where necessary, reviewed by Policy and Planning Branch to ensure the use is acceptable.
- Branches maintain a variety of additional safeguards including locking file cabinets and controlling physical access to records through human intervention.
- Computer applications are designed so that programmers cannot access personal data held by the system, once the system is operational. Data is only accessible by the designated users or by database analysts (not programmers) if required by the Branch.
- The Department continually works to improve systems security and to ensure that all use, access, and disclosure of personal information in systems is HIPA compliant.

As well the following organizational safeguards are in place:

- All employees are required to take an Oath of Office upon hire which includes an oath of confidentiality;
- All employees are made aware of the appropriate use policy for department technology and information systems;
- Systems are designed to limit access wherever possible to only those who need to know the information to perform their jobs; and,
- Staff are made aware that personal information is not to be shared except in accordance with policy or where approved by management in specific circumstances.

5. Health (continued)

Access to all computer technology is limited based upon user ID and password. Individuals are only given access to programs required for their specific work needs.

Saskatchewan Health is an active member of the ITO Security Charter Group and has signed the Charter.

OPENNESS

Health will provide information regarding the protection of personal information upon request and is available in many forms – verbally, paper, Internet. For example, information regarding the *FOI* process is available at the Saskatchewan Health website.

PROVIDING ACCESS

Saskatchewan Health falls under *The FOI Act* and complies with its rules regarding access to records. In addition, individual branches will provide access for specific information (e.g. patient specific physician billing records to the individual the information is about) in accordance with legislation and policy. Individuals are allowed to access any information about them in accordance with *FOI*. The *FOI* Unit in Policy and Planning Branch handles all *FOI* requests. Other branches may handle requests specific to their program areas and will only disclose in accordance with program and policy.

All personal information is identified in the *FOI* directory. Most personal information in the department is held in electronic databases accessible at an individual level through unique identifiers (such as Health Services Number) or by name. Some personal information may be contained in correspondence and may be more difficult to locate without sufficient direction.

With respect to the release of personal information, whether through the *FOI* process or otherwise, the Department takes steps to satisfy itself that the individual requesting the information has a right to access the information. For example, the Department confirms that the person is requesting their own information or has legal authority to access the information. Legal counsel provides advice if a request is unclear. A record of the release may be kept through copies or through a log. Through an *FOI* process a copy of the release and a log are maintained. Individual's accessing his or her own data will consent to its release.

When sharing information with other agencies, the other agencies are bound as follows: where information is disclosed to another government department in accordance with the law, the other department is bound by its own statutes

5. Health (continued)

including *FOI*. Individuals receiving information disclosed with consent will be bound by the specifics of the consent. Researchers receiving information (personal information is released only with consent) are required to sign a research agreement restricting use.

As described elsewhere, Saskatchewan Health maintains a range of personal information about individuals. Information will be updated but only if from an accurate source. Most major systems will track the change and keep a historical record. Information is not changed if it is clinical in nature. Rather, a file may be appended. *HIPA* provides strict rules regarding amending records.

CHALLENGING COMPLIANCE

The *FOI* Unit/Policy and Planning Branch is available for complaints about practices. Under *The FOI Act*, the Information and Privacy Commissioner has authority to address complaints. The Ombudsman also has authority to address complaints.

As reported in the media, the Department recently terminated a staff member for using personal information inappropriately. The individual used information that he/she had legitimate access to for a personal purpose which, the Department feels, violated departmental policy.

RECOMMENDATIONS

1. Health should formalize ongoing, mandatory training and re-enforcement of *The FOI Act*, *HIPA* and privacy principles.
2. It should be noted that *HIPA* provides the majority of the components of a privacy framework needed in Health once it (and the proposed amendments) is proclaimed. Health should assess the impact of the privacy framework that will be established by the government as a whole on the department and respond accordingly.
3. Based upon the sensitivity of the information determined by the data classification scheme developed by the government as a whole, additional safeguards should be placed on highly sensitive data.
4. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.

5. Health (continued)

5. Health uses the Saskatchewan Administrative Records System (SARS) and Operating Records System (ORS) to guide it in the retention and destruction of personal information. These policies should be reviewed with current privacy practices in mind. It should be noted that *HIPA* does give guidance in this area.
6. Health should ensure that regular reviews are completed to ensure compliance with *The FOI Act*, *HIPA* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
7. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
8. From a privacy stand point, the use of the Saskatchewan Health Card as a means of identifying individuals applying to government programs may be problematic. Since by definition health information is intimately personal, the Government, although Departments and Crown Corporations do not access health information per se, may wish to review the means used to ensure that an applicant is indeed a resident of Saskatchewan. The Government (and/or Health) may wish to consult with counsel to ensure compliance with legal norms or consider another means of confirming residency. The Government may also wish to enter into similar discussions with respect to the use of Social Insurance Numbers (SINs) as a means of identification.

6. Highways & Transportation

INTRODUCTION

The Department of Highways and Transportation does collect some personal information but it is not extensive in comparison to the other organizations reviewed. *The FOI Act, the Highway Traffic Act and the Highway & Transportation Act* govern the department. Personal information is accessed throughout the performance of typical activities in the following areas:

- Transport Compliance
- Fatal accident investigation
- Administration of the Trucking Partnership Program
- Information Technology databases and applications

The types of information collected include driver license information, safety inspections, traffic violation information and conviction information.

The Department shares information with and receives information from SGI and shares information with the Commercial Vehicle Safety Alliance (a safety association of North American jurisdictions using a common inspection methodology). It also partners with Saskatchewan Environment in a call centre through which Canadian Police Information Centre (“CPIC”) information is accessed. Saskatchewan Environment provides some resources to run the call center and shares the call center with Highways.

Transport Compliance accesses driver information from CPIC, SGI (i.e., carrier profiles, driver license and registration information) and internally developed databases (i.e., Commercial Vehicle Safety Alliance (CVSA) Inspection Information System, Traffic Ticket Information System (TTS) and the Complaint and Investigation Management System).

Fatal accident investigation operations staff in the regions investigate fatal accidents. The Department prepares a fatal accident report including an internal accident investigation form. SGI's motor vehicle accident (MVA) report form is attached to the Department's report. Highways uses the information on this form so that they may review road conditions, slope of road, etc. to identify any corrective actions they may need to take. This form contains personal information (i.e., driver's license and vehicle plate number) but this information is not used by Highways.

6. Highways & Transportation (continued)

Trucking Partnership Program Administration

The Trucking Partnership Program Administration Department performs an audit of a trucking company's compliance and safety record in the process of assessing their suitability as candidates for the Department's Trucking Partnership Program. Personal information is obtained on a driver's safety record and traffic convictions (excludes criminal convictions). This information is shared with SGI, the department's Transport Compliance area and Alberta Transportation (they have a similar partnership program) by request only. The personal information is stored electronically and as a paper copy and not contained within an internal database.

The Department uses *The FOI Act* to define personal information.

ACCOUNTABILITY

Ultimately, the Deputy Minister is accountable for privacy and the protection of personal information. The Deputy Minister approves any policy and Region Managers & Transport Investigation Managers oversee compliance as per policy. To date, the Department has not been asked by the public as to who this individual is.

The Department does not outsource any processing of personal information. The Department does have some written policies which include the CVSA IIS Computer System. This explains how Highway Traffic Officers are to use the system and that unauthorized use is not allowed. CPIC identifies that all information shall be guarded and considered confidential.

The Department does not have specific privacy policies and does not have employees sign confidentiality agreements beyond the oath of allegiance. Transport Compliance developed the CVSA IIS policy regarding access, use and security of personal information and the Department does follow *The FOI Act*.

IDENTIFYING PURPOSES

Highways uses the Saskatchewan Administrative Records System (SARS) Policy (as provided for in *the Archives Act*) and law enforcement practices to determine what personal information they maintain. They categorize personal information using *The FOI Act* definition. All personal information is stored in a secure manner and *The FOI Act* provides guidelines for law enforcement information.

Highways does not define the sensitivity of personal information other than what is provided in *The FOI Act*.

6. Highways & Transportation (continued)

Information is stored in network, password protected, databases and locked file cabinets. Multiple password levels and an internal firewall protect the Department's database systems.

The only personal profiles created by combining personal information from various sources is in the investigations complaint system from CVSA, TTS and the Carrier Profile Systems. Highways does not tell people in advance why their personal information is being collected and how it is going to be used as this is used for law enforcement purposes.

CONSENT

The Department does not gain consent from individuals when obtaining their personal information. In the Transport Compliance Branch, authority for receiving information is given through the various acts and law enforcement practice.

In the Transportation Partnership Program (TPP), consent to collect information from a third party is not gained from the individual. Any personal information obtained by the administrator in regards to the company being audited is released to that company.

LIMITING COLLECTION

The Department obtains only information that is needed through various forms. TPP informs employees verbally of proper conduct when dealing with information. The Transport Compliance Branch obtains information on law enforcement evidence forms, which are pre-printed with fill in the blank answers. Fatal accident investigation only receives motor vehicle accident reports (MVAs) for fatal accident investigation purposes.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

To ensure that the information is used for what it was collected for, TPP monitors all administrative staff closely to ensure proper procedures are used. TPP does not have policies in place for the retention or destruction of data. All information not in use is archived. TPP does collect information from sources other than the individual such as SGI and Transport Compliance CVSA database, Ticket database and Unix system.

The Transport Compliance Branch uses training, policy statements, public service oath or declaration of office and oath of police maintained by Justice to ensure the personal information collected is used for what it was intended. The

6. Highways & Transportation (continued)

branch follows *The FOI Act* and SARS for the retention and destruction of data. Any data that is no longer in use is shredded or erased. The branch does collect information from sources other than the individual such as Environment (CPIC), SGI, TTS and CVSA.

MAINTAINING ACCURACY

As a means to attempt to ensure that the information they collect and use is up to date and accurate, the Transport Compliance Branch and fatal accident investigation verifies questionable information by contacting the source of the information.

The TPP does ensure the information it collects and uses is up to date, accurate and complete through an audit process.

SAFEGUARDS

Information Technology Services (ITS) is responsible for the maintenance and servicing requirements of internal databases. The Department has identified specific logical and physical access controls used to protect information. For security purposes these will not be defined in this report.

ITS is responsible for the overall security and integrity of all the Department's electronically stored information. Several security measures and procedures exist to ensure the internal and external security of the information.

As the only information about an identifiable individual in a fatal accident investigation is the name provided on the SGI MVA form, Highways locks files in a filing cabinet.

Any employees, contractors or third parties who are sharing the information with the branch are required to sign confidentiality agreements. In order to improve privacy and security, the branch has assisted in developing government wide IT security policies. The branch, which is presently assisting in developing the governments IT Security Architecture, has discussed the merits of a penetration test and performed an internal evaluation of vulnerabilities.

TPP uses locked filing cabinets and logical security means to safeguard its personal information. TPP may use confidentiality agreements with employees, contractors or third parties depending on the type of information shared.

6. Highways & Transportation (continued)

The Transport Compliance Branch uses logical and physical security means to protect personal information. Organizationally, to protect personal information, employees are asked to provide a criminal record check for employment. Any individual who is sharing personal information is required to sign a confidentiality agreement and employees sign oaths. Access to private information is controlled by IT and database managers and business plans identify business needs.

OPENNESS

Transport Compliance communicates policies and procedures regarding personal information to the general public through *FOI* administration. TPP does not release personal information. Company information may be released to other government organizations with a confidentiality requirement.

PROVIDING ACCESS

As the Department is not the principle collector of primary personal information (e.g. driver information) neither fatal accident investigation or TPP have had requests from individuals.

The TPP will release audit results and general sections of contract agreements as part of administering partnership agreements. One individual does not handle all inquiries. Authorized staff handle these inquiries as needed. TPP is confident that they can identify all personal information. When releasing information, the information will only be released to agreement companies or authorized organizations within the agreement process. This is not accident information, which identifies other drivers – only the fact that there was an accident. If the authorization to release information is unclear TPP receives advice from the Director. Audit information that is released is recorded in the company file. If the information is released, any program company under review is notified of the review and consent is implied to release the information. The recipient of the information is contractually bound through the agreements, which may reference this. The program does not delete, update or amend information. The program requests the company partners to provide updated information. To confirm the information, the program goes through an audit process. When obtaining the information, partner companies obtain consent from individual employees.

Transport Compliance does allow individuals to access their personal information through *FOI* guidelines and CVSA. The freedom of information process is the process used to release personal information. The *FOI* administrator handles these inquiries including the consent, authority and release of information for the program.

6. Highways & Transportation (continued)

CHALLENGING COMPLIANCE

The Transport Compliance Branch has never had a complaint concerning personal information and, therefore, does not have a formal policy in place to deal with complaints.

TPP does have a formal policy in place when dealing with complaints about personal information

Fatal accident investigation does not have a formal policy in place to deal with complaints.

RECOMMENDATIONS

1. Highways should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. Highways should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. Highways should establish formal accountability for privacy within the department.
4. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.
5. Highways should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Given that the nature of the information held by the Department is relatively defined and static, this may not be a time consuming exercise for the Department. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. Highways should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used, retained or disclosed. The TPP program is a good example of this.
7. Highways should implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.

6. Highways & Transportation (continued)

8. Highways should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this overarching policy, each Branch should review its current policy to ensure alignment with departmental policy.
9. Highways should implement regular reviews to ensure compliance with *FOI* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
10. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
11. Highways should implement a system to record what information was disclosed, shared, etc., in order to inform an individual of the specific information about them that has been disclosed.
12. Highways should develop formal procedures to be followed to authenticate individuals when information is being requested, including techniques for in-person, written, electronic, IVR and call center requests.
13. As Highways does not use the name of the individual identified on the MVA form for fatal accident investigations, we recommend this information be blackened out on the form.

7. Information Services Corporation

INTRODUCTION

Information Services Corporation (“ISC”) collects personal information on behalf of the government of Saskatchewan for the purposes of recording land and personal property registry information.

ISC collects one or more of the following items pertaining to personal information of customers, clients or users of ISC information:

- Name
- Addresses
- Phone numbers
- E-Mail addresses
- Fax numbers
- Surveyor designation
- Sask Land Surveyors Commission Number
- Credit Card Number
- Date of Birth
- Generation
- Writs

Information is collected and entered into the Land Registry system by e-Business Services. Other groups within ISC subsequently access it in the system. The ISC Business Development and Marketing areas share personal information (name, address, phone numbers). The ISC Customer Help Desk shares information with other ISC groups in processing customer inquiries. Writ Registry Information, which is part of the Land Registry, is shared with the Personal Property Registry. Information contained in both the Land and Personal Property Registries is of public record.

In addition to the internal sharing of information noted above, ISC shares personal information with other government departments and agencies including the following:

- Change of ownership information is shared with municipalities or SAMA for tax assessment purposes.
- Ownership information is shared with the Farm Security Board.
- Ownership information is shared with Saskatchewan Industry and Resources.
- ISC currently receives personal information regarding tax liens/writs from the Department of Finance which goes to the Personal Property Registry.

7. Information Services Corporation (continued)

ISC also has an arrangement dating back to the 1940's with IHS AccuMap, a service provider to the oil and gas industry. Under this arrangement bulk land titles information is provided to IHS AccuMap.

ISC determines what is personal information based on adherence and reference to the *Freedom of Information and Protection of Privacy Act (The FOI Act)* and consultation or reference to one or more of the following groups, individuals or policies:

- ISC's manager of Risk and Security
- ISC's Freedom of Information Officer
- ISC's Security Management Committee
- Registrar of Titles
- ISC Security Policy
- ISC Human Resource Manual section entitled, "Acceptable Use of Information Technology"
- ISC Clean Desk Policy

With respect to personal information, ISC is governed by the following legislation:

- *The Freedom of Information and Protection of Privacy Act*
- *The Land Titles Act, 2000*
- *The Land Surveys Act, 2000*
- *The Personal Property Security Act*
- *The Crown Corporations Act*

One of the issues currently facing ISC is the sale of bulk information collected by ISC for the purposes of the Land and Personal Registries. This is an issue because various organizations have an interest in purchasing bulk information and it represents a source of revenue for ISC. Of particular concern is the sale of bulk registry information to business organizations that may use the information for purposes, which certain individuals may take issue to, such as using the information for the purposes of marketing. ISC has established a Privacy Committee and is working to establish a privacy policy relating to this issue. To date ISC has received two outside legal opinions relating to privacy and ISC continues to research this matter.

7. Information Services Corporation (continued)

ACCOUNTABILITY

At ISC a number of different committees and individuals are accountable for managing the policies regarding personal information and overseeing compliance including the following:

- The Privacy Committee comprised of the Vice President of Customer Services and the Assistant Vice-President of Marketing are responsible for reviewing all requests or proposals that relate to the sale of personal information collected by ISC for the purposes of the Land and Personal Registries.
- The Freedom of Information Office processes, coordinates and tracks all freedom of information requests.
- The Manager of Risk and Security oversees corporate security and is responsible for compliance with ISC Security Policy, ISC Human Resource Manual section entitled “Acceptable Use of Information Technology”, ISC Clean Desk Policy, ISC Incident Reporting Process and ISC Mandatory Display of Photo Identification Policy and Procedures.
- The Director of E-Business Services oversees policies and security of Client Account Management System, Client Entry Management System, Client Image Management System and Client Output Management System.
- The ISC Security Management Committee, of which the Manager of Risk & Security is a member, deals with all security related matters including issues, incidents and breaches of security. The Committee also is responsible for updating the ISC Executive group on these matters.
- The Registrar of Titles is responsible for overseeing compliance with all aspects of land registry.
- The Personal Property Registrar is responsible for overseeing compliance with all aspects of the Personal Property Registry.

The identity of the above individuals is made known to the public upon request.

An agreement is in place with a third party to protect the processing of credit card transactions. ISC also has other confidential processes in place to protect credit card information.

ISC has the following policies in place which deal with personal information:

- ISC Security Policy
- ISC Human Resource Manual section entitled “Acceptable Use of Information Technology”
- ISC Clean Desk Policy
- ISC Incident Reporting Process
- ISC Mandatory Display of Photo Identification Policy and Procedures

7. Information Services Corporation (continued)

ISC does not have one single policy specifically devoted to the privacy of personal information.

The following policies have not been formally developed; however, they are followed informally and/or are targeted for formal completion by the end of 2003:

- Expansion of Saskatchewan Administrative Records System within ISC to ensure compliance with *The Saskatchewan Archives Act* and the *Freedom of Information and Protection of Privacy Act*
- ISC Senior Management is working on developing a privacy policy to deal with the bulk sale of personal information collected for the Land and Personal Property Registries

ISC makes its policies available publicly.

ISCs policies were last updated in May and June 2002.

ISC has communicated its policies to staff through email and the policies are available to all employees on ISC's network. Training sessions have been conducted for Finance and Administration, Corporate Development and ISC Managers and Directors. Other staff groups have not received formal training to date.

In addition to policies and procedures currently in place all employees sign an "Oath of Office". Also, ISC now periodically has as part of its system log in script the following statement, which staff must agree to in order to log on the system:

"By selecting OK, you acknowledge and accept that the tasks performed on this computing device are logged and may be monitored. In addition, you acknowledge that you are familiar with and agree to abide by all ISC policies, and the terms and conditions of employment."

ISC limits staff access to personal information based on the user's need to access information.

ISC has established procedures to receive and respond to complaints and inquiries in compliance with Freedom of Information Act requirements. Complaints and unusual inquiries are handled by ISC's Incident Reporting Process.

7. Information Services Corporation (continued)

Compliance with ISC's policies and procedures are monitored through the following up on complaints, control and monitoring of access to information maintained in the Registrar's Office. e-business has requested that an internal audit be completed on Client Account Management System and a general compliance review on ISC's policies and procedures. The dollar budget has been determined and performance of the audit is planned for the fall of 2002 or in 2003.

ISC staffs its own Call Centre, which is currently considering putting in place a "call monitor" position. That person would be responsible for monitoring call center calls to not only monitor compliance with ISC's policies and procedures but also ensure the level of customer support provided is at a high level.

IDENTIFYING PURPOSES

ISC considers the following in determining what personal information to maintain:

- Legal and Legislative requirements
- Internal policies, processes and program requirements
- Saskatchewan Administrative Records System
- *Saskatchewan Archives Act*
- Collection and retention of publicly searchable information based on *The Land Titles Act, 2000* establishing the registry as a public registry
- Collection and retention of publicly searchable information in the Personal Property Registry
- Other personal information collected for correspondence and consultations in order for ISC to carry on its business

ISC has not developed nor implemented its own information classification system that identifies the type of personal information collected and its sensitivity. This is considered a long-range plan for consideration once time and resources can be allocated. In the interim ISC has communicated to staff via email that ISC will follow the guidelines as outlined in the Canadian Public Sector Security Classification Guideline prepared by the National CIO Council Subcommittee for Information Protection. To date this Guideline has not been widely followed at ISC.

ISC's most sensitive information (credit card information as an example) is physically secured in locked cabinets in a locked room. Highly sensitive electronically stored information is password protected and can be accessed by a

7. Information Services Corporation (continued)

limited number of authorized ISC personnel. Individuals responsible for areas that use sensitive information include the following:

- Vice President of Customer Services
- Chief Information Officer
- Chief Financial Officer
- Registrar of Titles
- Director of E-Business Services
- Manager of Customer Call Centre
- Controller of Surveys
- Team Lead, Security Operations

Customer profiles are created in the Opportunity Development Framework group and by the HP Service Desk (help service desk).

Clients must complete forms with information as required by Act and Regulations for new information collected for the purposes of registration in the Land Registry and Personal Property Registry.

At the customer call center, if clients ask, they are informed that personal information is collected to populate the ISC customer database for ease of use when calling back. Otherwise consent is considered to be implicit.

Regarding personal information and the implementation of new business processes, ISC is currently assessing obligations to clients respecting personal information provided for registration purposes. Specifically ISC is considering the release of bulk registry data. As part of ISC's ongoing assessment the Corporation is considering the following:

- Internal and external legal opinion
- Review by the Manager of Risk and Security
- Guidance from a committee of senior management, who are developing a Privacy Policy

When new technology enables potential for additional services ISC seeks legal opinion to ensure privacy rights are maintained.

ISC Customer Service Centre and Call Centre employees are trained in dealing with all customer inquiries, including how personal information is going to be used, through training courses, instruction manuals and instruction sheets.

7. Information Services Corporation (continued)

CONSENT

Verbal implied consent is given when clients voluntarily provide personal information through utilizing the help desk. Land transactions require authorizing signatures on submitted information, which is implied consent and acknowledgement. Consent to collect information is considered to be implicit in applying to the Land or Personal Property Registry as these are public registries containing certain personal information mandated by Act or Regulations.

Electronic and paper forms are maintained electronically and in hard copy. A high number of phone calls are recorded in the service desk database.

Completion of electronic forms through the web site require acceptance of “Terms and Conditions”. Land transactions require authorizing signatures on submitted information, which is implied consent.

ISC monitors the use of personal information to ensure adherence to the *Land Titles Act 2000*, section 77. Regarding the release of bulk data, as previously discussed, ISC has sought legal opinion and has established a Privacy Committee to deal with this issue.

Currently ISC does not inform individuals and gain their consent prior to disclosing personal information to third parties when searches are conducted in the Land Registry or Personal Property Registry. Information contained in these Registries is considered to be public information. ISC continues to discuss and consider this issue when dealing with information gathered for the purposes of Land and Personal Property Registry. Currently ISC provides bulk Registry data to municipalities and the Farm Security Board without consent. As previously noted, the release of bulk information is a concern, particularly when the recipient of the information may use that information for purposes, which may be questionable in the public’s mind.

LIMITING COLLECTION

In order to ensure that only personal information that is needed is asked for, ISC has developed internal policies and procedures addressing the issue. Internal reviews monitor compliance. Information collected is based on legislative and regulatory requirements to establish and maintain the public Land and Personal Property Registry. Standard forms are used for the collection of most information to help ensure only the appropriate information is collected.

Other information collected through correspondence and consultation is used to respond to clients through the Registrar’s Office.

7. Information Services Corporation (continued)

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

ISC ensures personal information is used only for the purpose it was originally collected through adherence to the *Land Titles Act, 2000*, section 77, through ISC's Incident Reporting Process, and through the communication and enforcement of the following:

- ISC Security Policy
- ISC Human Resource Manual section entitled "Acceptable Use of Information Technology"
- ISC Clean Desk Policy

ISC has formal policies in place to deal with the retention and destruction of information including the following:

- All hard copy registry information is retained. Images of registry information is available for public viewing
- Internal documents are retained for later reference and archiving
- ISC Security Policy
- ISC Human Resource Manual section, "Acceptable Use of Information Technology"
- ISC Clean Desk Policy

The following policies have not been formally developed, however, are followed informally and/or are targeted for formal completion by the end of 2003:

- Development of an "operating records system" schedule
- Expansion of Saskatchewan Administrative Records System within ISC to ensure compliance with *The Saskatchewan Archives Act* and the *Freedom of Information and Protection of Privacy Act*.
- ISC Senior Management is working on developing a privacy policy to deal with the bulk sale of personal information collected for the Land and Personal Property Registries

ISC does not collect personal information about an individual from anyone other than him or her except in the following cases:

- Reference checks are performed for credit applications (with written consent from the client)
- Applications to the Registry may be completed/submitted by an agent (e.g. lawyer)
- Correspondence and consultations may be by an agent

7. Information Services Corporation (continued)

MAINTAINING ACCURACY

Information is verified each time there is a transaction involving the land and/or personal property registry.

Integrity of the Registry is integral to ensure that personal information as provided is properly recorded in the Registry. ISC cannot ensure that subsequent changes to personal information (for example a change of name by a title owner) are recorded unless ISC is so advised. Land and Personal Property Registration is voluntary; however, to encourage accuracy of information in the Registries ISC has made standard forms available on its website to facilitate recording changes of personal information.

SAFEGUARDS

ISC has implemented a number of policies and initiatives, which have been communicated to staff, to protect personal information from unauthorized access, disclosure, copying, use or modification. For security purposes these will not be defined in this report.

The Provincial Auditor has recommended that agencies have employees agree periodically in writing with their security responsibilities. ISC anticipates to have this initiative implemented by the end of September 2002.

ISC has a number of logical and physical security measures in place to protect personal information. Organizational methods in place to protect personal information (including policies and procedures previously discussed) include limiting access to information on a “need to know” basis. Contractors and other third parties with whom personal information is shared are required to sign confidentiality agreements.

OPENNESS

ISC communicates its policies and procedures regarding personal information to those who request it or the general public through the following means:

- Access to information contained in the Land and Personal Property Registries is available to the public.
- ISC adheres to and communicates all provisions of the following:
 - *The Freedom of Information and Protection of Privacy Act*
 - *The Land Titles Act, 2000*
 - *The Land Surveys Act, 2000*
 - *The Personal Property Security Act*
 - *The Crown Corporations Act*

7. Information Services Corporation (continued)

- Copies of statutes governing ISC are available on the Queen's Printer website

PROVIDING ACCESS

Individuals are allowed access to their personal information contained in the Land or Personal Property Registries.

In order to release personal information ISC follows the process outlined in the *Freedom of Information and Protection of Privacy Act*. As well, the process for handling all information is outlined in ISC Security Policy and ISC Human Resource Manual, section "Acceptable Use of Information Technology".

Information routinely released to persons using the Land or Personal Property Registries includes their name, address, phone number, fax number, email address, client number and the applicable information contained in the Land and Personal Property Registries.

Individuals handling inquiries include Common Entity clerks, Customer Service Representatives or Call Centre Representatives. Searches of the Land Registry can also be performed over the Internet.

The release of information is handled by:

- ISC website search
- Staff-assisted searches at a Customer Service Centre
- Requests by fax or letter, signed by requestor, with a fax or hardcopy response

Client's performing ISC website searches are given a client number and password and are required to provide their client number and password before they can proceed with a search.

If authority to release personal information is unclear one or more of the following individuals or groups could be involved to review and determine if release is authorized:

- The Manager of Risk and Security
- The Freedom of Information Officer
- ISC's Security Management Committee
- Registrar of Titles

7. Information Services Corporation (continued)

ISC keeps record of the information released including the name of the recipient and the date released. More specifically FOI request records are maintained on file. All requests brought to the attention of the Manager of Risk and Security and the Security Committee are maintained on file. All Land Registry searches are electronically recorded. Any other information released is recorded.

Any information released is information from the Land and Personal Property Registries, which are public registries and may be searched as such. ISC business partners, suppliers, customers, and other business associates are made aware of data confidentiality responsibilities through non-disclosure agreements in contract wording. Where bulk data is released (e.g. to municipalities or the Farm Security Board) ISC has wording in the bulk data agreement restricting the redistribution of the information.

ISC will amend an individual's personal data where it is shown to be inaccurate, incomplete or out-of-date. In order to amend data ISC requires evidence that meets regulatory standards. For the Land Registry confirmation of changes are sent to the client. This does not occur with the Personal Property Registry.

CHALLENGING COMPLIANCE

ISC has an Incident Reporting Process in place to deal with complaints about its personal information management practices or policies. ISC has received one complaint since the beginning of this review – a credit applicant whose application was faxed to a reference for the application to provide proof that ISC was authorized to be checking the reference.

ISC has changed their process to prohibit the faxing of information that may be considered personal.

RECOMMENDATIONS

1. ISC should provide ongoing, mandatory training and formal re-enforcement of the FOI Act and privacy principles.
2. ISC should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. ISC should establish formal accountability for privacy within the Crown Corporation.
4. In the development of contracts with outside parties, ISC should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the corporation provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the corporation's personal information (privacy) requirements.

7. Information Services Corporation (continued)

5. ISC should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. ISC should ensure that regular reviews are implemented to ensure compliance with FOI principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
7. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
8. A formal process should be put in place to ensure that when staff change roles within the organization the individual's system access is updated to match their new access to information requirements.

8. Justice

INTRODUCTION

The Department of Justice (Justice) retains overall responsibility for two large, yet varied aspects of law and order within the province. The first deals with Criminal Justice while the second addresses Civil Law, Public Law and the remainder of the non-Criminal Divisions within the Justice Department.

Justice - Criminal is comprised of various Divisions, each of which sets its own standard for collection, retention, disclosure and destruction of personal information. Among these are Law Enforcement Services, the Provincial Court Payment Information Centre (PCPIC), Court Services, Policy, Planning and Evaluation, Community Services, and Provincial Prosecution Services. There is considerable sharing of information among the elements of Justice as well as with non-Justice departments (such as SGI, the Department of Social Services, Department of Labour) and agencies (such as Worker's Compensation Board, Health Canada, RCMP).

Similar to Justice - Criminal, Divisions within Justice - Civil have been created. These include Policy, Planning and Evaluation, Family Justice Services, Pension Benefits, Consumer Protection, Public Guardian and Trustee, Queen's Printer, Human Resources, Civil Law and Corporations Branch. Each collects personal information and in many instances, information is shared with and received from internal and/or external government entities. Any non-public information, which identifies, or tends to identify an individual, is considered to be personal information, as per the *Freedom of Information and Protection of Personal Information Act (The FOI Act)* definition. A considerable amount of information received by Justice, although not necessarily falling squarely within the definition of personal as per FOI, is treated as confidential.

In addition to *The FOI Act*, Justice is governed by numerous statutes which require that personal information be collected and shared. For example, Prosecution Services is required by law to disclose to the accused all relevant information, whether or not it happens to fall into the category of personal information, pertaining to a given criminal prosecution, pursuant to the *Canadian Charter of Rights and Freedoms*. In addition, the court may order that particular information be sealed or disclosed. All lawyers are governed as well by the Code of Professional Conduct of the Law Society, the Queen's Bench Rules and Rules of Court.

In addition to governing legislation, confidentiality agreements are required by the Dispute Resolution Office as part of its mediation process. The Public Guardian and Trustee has a legal relationship with its dependent adult clients

8. Justice (continued)

and as administrator of deceased estates. As such, the Public Guardian and Trustee stands in the place of the Office's clients and acts in their best interests. This legal relationship establishes the criteria by which all decisions affecting the Office's clients are made, including those around privacy and consent.

Most Divisions of Justice rely on the knowledge and experience of employees with respect to the circumstances under which personal information may be disclosed. Victims Services, however, has implemented internal policies to regulate the use of personal information. Employee training with respect to personal information is sporadic.

ACCOUNTABILITY

Each Division has identified the responsibility center within it for the management of policies pertaining to personal information. The identities of these persons are made known to the public to ensure appropriate access.

Some outsourcing of IT programming and systems support does take place. In addition, some Divisions also outsource some pieces of work, for example, court transcripts, which are public documents except where the transcript relates to a young offender or where there is a publication ban in place. Justice requires that in all IT outsourcing situations, a confidentiality clause be incorporated into the contractual arrangement in order to protect the confidential nature of information held by the Department. All professionals accessing personal information are governed by their respective professional code of conduct.

Justice does not rely on codified policies and procedures, but rather make use of informal arrangements and cultural norms to employees FOI requirements re the handling of personal information. Some Divisions have implemented written policies. These Divisions include the Public Guardian and Trustee, Family Justice Services, Corporations Branch and the Queen's Printer. These documents are available to the public.

For the most part, Divisions orally communicate policies and expectations with respect to the handling of personal information to new employees as part of their orientation process. In many Divisions, personal privacy issues are often raised and discussed during staff meetings. Discussion of personal privacy issues is also raised with identified positions, i.e. positions seen as having a need for such training, as part of their ongoing training requirement. Privacy issues are also discussed in the Department's Employee Orientation Manual, to which employees are free to refer as necessary. It should be noted that the Employee Orientation manual is currently undergoing revision. Although high level policy and procedures are set out in Justice manuals, most Divisions candidly admit they are lacking in specific policy and training with respect to privacy issues.

8. Justice (continued)

Of note as well is the fact that a Memorandum of Understanding (MOU) has been signed between the Canadian Council of Insurance Regulators and the Canadian Securities Administrators (which includes the securities regulators of Saskatchewan). This MOU deals with mutual co-operation in the regulation of persons coming under the jurisdiction of securities and insurance authorities and, as law enforcement entities, to enforce the laws related to that regulation. The MOU sets out the framework for the sharing of information between and among such agencies. It is noted in this report as an example of a potential mechanism through which information pertaining to individuals might be shared inter-Departmentally to ensure that FOI principles are recognized and maintained.

All Divisions restrict access to personal information, with sensitive material kept under lock and key. Electronic information is protected by passwords and firewalls, none of which is technologically failsafe. Justice does not presently retain a policy with respect to the means by which to identify and categorize the sensitivity of a particular document or the requirements in terms of the level of sophistication of physical security and storage required.

Third parties required to access personal information as part of their duties are not as a rule required to sign a confidentiality agreement and are dealt with on a case-by-case basis. For example, all outsourced information pertaining to a Victims Services survey must be disclosed upon completion of the survey. All outsourced IT contracts contain a standard "Agreement of Confidentiality and Security between Saskatchewan Justice and Employees or Principals of Private Companies".

Steps have been taken to ensure that employees are cognizant of the requirements of FOI, however, little policy is in evidence to which an employee may refer for guidance.

For example:

- Court Services has completed a handbook discussing access to information contained on young offender files and a written policy on access to Sheriff's files
- Rules of court set out procedures for access to family law files.
- Provincial and superior courts have implemented rules for public access to the court record
- Law Enforcement Services has implemented a written set of policies for coroners

8. Justice (continued)

Training is ongoing, however, the reliance on expertise and experience and the lack of specific policy may have a detrimental effect on the ability of employees to be certain of their decisions regarding personal information. All government employees are required to take an oath of confidentiality upon joining the civil service. It is believed that these oaths are not regularly reviewed or explained in detail to employees subsequent to employment. No annual sign-off takes place to ensure that employees are aware of mechanisms for handling personal information.

A wide range of professional and program staff deal with requests for access to personal information. Regular employee supervision is the sole means utilized to monitor compliance with the principles of FOI.

IDENTIFYING PURPOSES

Only information which is integral to the business of the justice system or that is mandated by legislation is collected and retained. It is noted that Law Enforcement Services segregates information concerning deceased persons and police discipline files, however, no specific criteria are set out to ensure that the information collected is indeed relevant and necessary for the particular purpose.

Personal information is not segregated according to its sensitivity nor is a standard classification system in use within the Department. Documents containing personal information such as pre-sentence reports, victim impact statements or psychological assessments are not made available to the public without judicial authorization.

Personal information which is retained is automatically considered to be sensitive and is secured and locked. Access to offices in which such information is stored is restricted. Electronic information is protected using passwords and firewalls.

Clients of most Justice Divisions are informed as to the reason their personal information is collected. Justice – Civil Divisions creates personal profiles in Maintenance Enforcement on clients by aggregating information from various sources to fulfill its statutory role.

No specific training takes place to ensure employees are aware of FOI and other privacy requirements. Training with respect to privacy issues is *ad hoc* and irregular. No Departmental policy is in place to address this issue.

8. Justice (continued)

Justice – Criminal does create personal profiles using personal information collected. This information is shared among other interested and involved departments. For example, some branches have made use of personal information collected by another department to update its address files. Prosecutors compile dangerous offender information sheets by collecting information from police agencies and from Corrections files. When information is collected, the person providing his or her information is usually not advised as to the use for which it is being collected.

Security risks are assessed when new processes are being designed and implemented, as per the *Government of Saskatchewan Information Technology Framework* and the *Security Charter*.

CONSENT

Consent is not always obtained prior to collecting personal information. It is the view of Justice - Criminal that consent is not required or feasible in the majority of criminal justice and police matters. Victims Services does require a waiver from its clients with respect to survey requests and compensation claims information. Little monitoring is in place to ensure compliance with guidelines and regulations.

Justice – Criminal re-obtains consent prior to disclosing personal information outside the global justice system, however, such an occurrence rarely takes place.

Justice – Civil does obtain specific consent as necessary prior to collecting personal information. Some Divisions, such as Family Justice Services and the Dispute Resolution Office, require the consent of the individual to collect the personal information required, while others, such as Consumer Protection, Corporations Branch and Pension Benefits, view consent as being implicit when contacted by an individual.

When required, specific consent is either defined on the request form or application, or, if applicable, on mediation agreements. In some instances, Divisions do not obtain consent in circumstances in which they view obtaining consent to be unfeasible, for example, when Justice acts in its role of Public Guardian and Trustee, a dependent adult for whom the Public Guardian and Trustee acts is not legally capable of giving consent.

8. Justice (continued)

No monitoring takes place to ensure that information is used according to the consent obtained. Divisions view this as largely unnecessary because information is collected and used only once. Again, no discussion seems to have taken place surrounding the use(s), if any, made of the information if it is entered into a searchable data bank.

When personal information is collected, the individual involved is generally informed that the information may be disclosed to third parties as necessary. Public Law division does seek express consent by letter before any such information is disclosed to a third party.

LIMITING COLLECTION

Information is collected only if it is relevant to particular matters or to the ongoing work of Justice. There is little evidence that collection is monitored or that regular training is imparted to provide guidance to employees.

Corporate culture and past practice is relied on in many instances to guide the Department in limiting the information it collects. No specific policy has been implemented. Monitoring takes place through supervision of staff and ensuring that staff members are aware of their responsibilities vis-à-vis personal information security.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

Justice is of the view that only relevant information is collected and ensures that personal information is only used for the purpose for which it was collected by placing reliance on employee integrity and honesty. Many Justice professionals are also governed by their own professional codes of conduct and ethics. In some instances, departments use regular staff meetings and employee monitoring as forms of control. Controls are implemented in an *ad hoc* fashion. No specific policies or procedures are in place to govern use, disclosure, collection and retention of information.

Retention of information and destruction of records is governed by the *Archives Act* (Saskatchewan) and the Saskatchewan Administrative Records System (SARS).

Many Divisions of Justice collect personal information from police and other agencies. Justice is of the view that such collection is authorized by FOI and by accepted guidelines and practice.

8. Justice (continued)

MAINTAINING ACCURACY

Most information is obtained from the individual him or herself and is, therefore, presumed to be accurate. Other information is obtained through contact with family, friends or other sources close to the individual involved and is, therefore, also presumed to be accurate. Justice has no specific program or policy in place to require that information be verified through random and irregular checks. No regular audits are conducted to monitor accuracy.

SAFEGUARDS

Access to paper records is restricted during work hours where sensitive paper records may also be retained under lock and key. Records are kept under lock and key after hours. Electronic information is accessible only to selected persons, using passwords and firewall protection. The public has no unsupervised access to sensitive areas of Justice offices.

No specific policy exists to ensure the protection of personal information when new technology or processes are introduced into the Department.

Personal information is accessed by Justice employees on a need-to-know basis. Any unusual external requests for information are referred to supervisors within Departments. In situations, which are unclear or uncertain, advice is sought from Civil Law Division. No policies are in place to assist employees in determining the level of sensitivity to assign to a given document, nor the appropriate means of securing such a document.

As noted *supra*, some Divisions require confidentiality agreements (e.g. Office of Dispute Resolution) with outside third party contractors, however, no such agreements are required as between Government Departments or with the Divisions of the Department.

All Government employees sign an Oath of Confidentiality when hired, however, no annual sign-off takes place to reinforce the notion of the protection of confidentiality of information within the Department.

Ideally, Justice would like to put in place a program requiring background checks on employees, however this is not possible in many cases because of Collective Bargaining Agreements. It is unknown whether a need for such checks has been identified or whether the security of information in the hands of the Government of Saskatchewan is jeopardized because of the lack of information. All employees of the Government of Saskatchewan must take an oath of confidentiality at the time of hiring.

8. Justice (continued)

Systems Branch has worked closely with the ITO in developing 2 documents, which are fundamental to IT security:

- Government of Saskatchewan Information Technology Security Framework, and
- Government of Saskatchewan Security Charter

An executive has also been appointed to take responsibility for IT security policy for Justice.

Work is continuing to meet the recommendations of the Provincial Auditor's 1999 and 2002 Reports.

OPENNESS

Divisions refer members of the public to *The FOI Act* to explain the Department's privacy policies or procedures. As well, most guidelines and processes for access to information are communicated orally to the public pursuant to requests. Some information is available on the Internet with respect to finding the appropriate department/location where the information sought may be held, requesting information and the steps which may be taken in the event such a request is denied. Detailed policies covering consent, handling of information by the Department, retention and destruction policies are not yet available on the Internet.

PROVIDING ACCESS

Most Divisions of Justice do allow individuals to access their own personal information held by Justice. Information requested pursuant to FOI is governed as per the Act itself. Prosecution Services, is required to disclose relevant material to an accused/litigant as part of the criminal disclosure/civil discovery process. Some information is not disclosed, for example, adoption records.

The types of information normally released (as per the type of information held by a given Division) include financial and payment information, mediation summaries, names and addresses of corporate directors, officers, attorneys and shareholders. Some Divisions, such as Consumer Protection, Public Law, Civil Law and the Queen's Printer, do not release any information. The recipient is free to use the information as he or she sees fit.

Typically, no one individual handles all requests. As noted *supra*, no specific policies or procedures have been implemented, nor is regular and focused training mandated.

8. Justice (continued)

Justice has confidence that staff members are able to identify personal information. No specific policy or training has been implemented to assist or provide guidance to Justice staff with respect to the identification and collation of all information held by the Divisions within Justice with respect to an identifiable individual, should that individual request all information held pertaining to him or her.

Justice updates individual files as new or amending information is received. No process is in place to regularly monitor files and confirm content. Attempts are made to confirm new or amending information with the individual concerned, however, amendments may be made without the confirmation or consent of the individual to whom the information relates.

Requests are dealt with at as low a level as possible. Justice has confidence in the ability of all staff to recognize personal information and handle it accordingly. No specific policies have been implemented in this regard.

CHALLENGING COMPLIANCE

Some Divisions of Justice, notably Court Services, PCPIC and Prosecutions have a procedure by which an individual may challenge information management practices or policies. In other Divisions, complaints are received and handled on an *ad hoc* basis. The perceived seriousness of the complaint dictates the hierarchical level at which it is handled.

No specific policy exists to assist/guide employees in the determination of the appropriate level. None of the Divisions have reported having received any complaints in the period July 2001 – June 2002, however, Court Services notes that most inquiries have been received from the media seeking access to additional case information as well as from individuals who are involved in one way or another with cases which have come under public scrutiny.

One incident has taken place over the past twelve months in which a volunteer working in a Division of Justice allegedly obtained and misused personal information. The allegation was investigated and was determined to be completely without foundation.

RECOMMENDATIONS

1. Justice should ensure that policies and procedures are in place within all Divisions to ensure employees are provided with guidance and direction with respect to *FOI* requirements for handling personal information. Informal and ad hoc processes should be formalized, documented and the documentation readily available.

8. Justice (continued)

2. Justice should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act*, any other relevant legislation and privacy principles so that employees are aware of their obligations with respect to the handling of personal information.
3. In addition to the Departmental coordinator, an Access to Information coordinator should be appointed for each Division of Justice.
4. Justice should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
5. Justice should establish formal accountability for privacy within the Department as they have done with *The FOI Act*.
6. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.
7. Based upon the sensitivity of the information that it holds, Justice should consider the viability of implementing a policy of requiring background checks on employees having access to sensitive information, personal and otherwise.
8. Appropriate Memoranda of Understanding (MOU) pertaining to the handling and dissemination of personal information should be entered into between Justice and all agencies with which it receives or shares such data. Any such MOU must also be examined to ensure compliance with *the FOI Act* and with CSA . MOUs should include an assurance that any information passed is accurate, up-to-date and that it is either subject to specific and informed consent or that the information is identified as falling within an identifiable exemption under the legislation.
9. Justice should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
10. Justice should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. Regular monitoring should take place to ensure that personal information is used as per the consent obtained.
11. Justice should continue to implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.

8. Justice (continued)

12. Justice should ensure that regular reviews are implemented to ensure compliance with *FOI* principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
13. Justice should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this overarching policy, each division should review its current policy to ensure alignment with departmental policy.
14. All employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

9. Learning

INTRODUCTION

Saskatchewan Learning provides both teacher and student services. The Office of the Registrar administers policies related to credit requirements for secondary level completion; grade 12 departmental examinations; maintenance of a central registry of students at the 10, 11 and 12 levels for the purpose of transcript production; and teacher certification and accreditation. In addition, student services maintains demographic and enrollment information on K-12 students in the province.

In addition to teacher and student services, the Department is involved with various funding programs including the Student Loan program and employability assistance programs.

At Saskatchewan Learning, the following personal information is requested, as required, on a program-by-program basis. For example, a Health Services Number (“HSN”) is requested from Learning clients who require child health benefits from the Department of Health or when funding to the client is impacted by the number of client dependents. Social Insurance Numbers (SINs) are only collected for clients involved in joint programs with HRDC under the Labour Market Development Agreement (a Federal Government agreement, which requires SINs) and for teachers for superannuation purposes. Learning is very careful to ensure that the collection and usage of HSN or SIN information is controlled. To ensure that the Department is not in violation of any legislation governing the collection and use of such information, the Department of Justice has reviewed and approved Learning’s policies and procedures related to this information. Information collected is as follows:

- Full name
- Date of birth
- Gender
- SIN
- HSN
- Marital status
- Drivers License number
- Drivers License class
- Date of death
- Employment insurance status
- Social assistance recipient status
- Education attainment
- Citizenship
- Language of service

9. Learning (continued)

- Language of intervention
- Addresses
- Phone
- Email
- Parental income
- Financials
- Education history
- Employment history

The following personal data elements are self-declared. However, for specific funding programs (e.g. Student Loans Special Incentive Program and Employability Assistance for Persons with Disabilities) aboriginal or disability information is required to administer the respective program:

- Aboriginal status
- Disability status
- Visible minority

Note: The Saskatchewan Human Rights Commission was contacted for advice and guidance on questions related to personal information re: aboriginal, disability and visible minorities.

The Provincial Examinations, Student and Teacher Services branch collects both student and teacher information. The branch collects demographic and enrollment information on K-12 students in Saskatchewan as well as credit information for secondary level students. It also collects teacher information such as birth certificates, social insurance number, change of name certificates, marriage certificate, evidence of education, address, evidence of employers and salary, and limited medical information.

Saskatchewan Learning collects personal information on behalf of other government departments, agencies or levels of government. Through Saskatchewan – Canada agreements, the Department collects personal information required for the federal government's HRDC Department for the Labour Market Development Agreement (LMDA- effective February 6, 1998) and Canada-Saskatchewan Integrated Student Loans Program.

Saskatchewan Learning shares personal information with other groups or sections within the organization. Personal data, within the common individual registry, is shared across departmental business areas for the administration of specific programs to common clients.

9. Learning (continued)

The Provincial Examinations, Student and Teacher Services branch shares Student Financial Assistance information with other government agencies as well as student information with Apprenticeship and Trade Certification. The branch shares teacher information with the Official Minority Language Office, Regional Offices, School Grants, Curriculum and Instruction Branch, Special Education Unit, Teachers Superannuation Commission, STF, SSTA, School Divisions, other provincial and state departments of education, universities and teacher exchange authorities.

Saskatchewan Learning also shares personal information with other government departments or agencies. Personal data is shared with other departments for the administration of specific programs to common clients. For example, these other agencies and departments include, service providers responsible for dispersing and collecting student loans, the federal government to conduct program evaluations, and for verification of assessment information, data is exchanged with Saskatchewan Government Insurance, and the Departments of Health and Social Services.

All data exchange arrangements require approval and documentation (i.e. Memorandums of Understanding and Data Sharing Agreements), including review and approval by the Department of Justice to ensure the Memorandums or Agreements are in compliance with legislation and court rulings. This process is necessary to ensure that all parties are informed and have an understanding that only required data is to be shared for the administration of a specific program or service with reference to particular governing acts and regulations (e.g. *The Freedom of Information and Protection of Privacy Act (The FOI Act)*).

Once developed, these documents are vetted through Justice and executive directors, responsible for the specific program, for approval. An example, of an approved data sharing agreement, is the agreement between SGI and the Department's Student Financial Assistance Branch. Both parties have approved this agreement and IT development is underway to implement this exchange, which is scheduled for December 2003.

Saskatchewan Learning receives personal information from other departments and agencies. Memorandums of Understanding ("MOU") or Data Sharing Agreements are developed whenever the sharing of personal information is required to administer specific programs to common clients. The Department exchanges personal information with other organizations, where MOUs or data sharing agreements exist, as in the following examples:

- Human Resources Development Canada: LMD Agreement (February 1997, Annex 6: *Arrangements for the Exchange of Information and Data*)

9. Learning (continued)

- Department of Social Services and Provincial Training Allowance: Memorandum of Understanding (October 1997, Revised December 1998, 2nd Revision March 2001)
- Department of Health and Provincial Training Allowance: Memorandum of Understanding to nominate PTA clients for supplementary Health Benefits (January 2000)
- Saskatchewan Government Insurance and Student Financial Assistance (June 2002): Data Sharing Agreement to verify client eligibility

The Provincial Examinations, Student and Teacher Services branch receives student information from schools and school boards (includes independent schools and band schools) and receives teacher information from school boards (includes independent schools and band schools), universities, other provincial and state education officials, teacher exchange officials and disciplinary information from the STF.

Saskatchewan Learning defines personal information as personal information about an identifiable individual that is recorded in any form and included in Saskatchewan's *Freedom of Information and Protection of Privacy Act*, (Part IV, Section 24, subsections (1) and (2)).

The Provincial Examinations, Student and Teacher Services branch defines personal information as per the *Freedom of Information and Protection of Privacy Act*.

The province's *Freedom of Information and Protection of Privacy Act* (FOI) specifies the legislation governing the Department in respect of personal information. There are other acts and regulations that are taken into account when planning to collect, use, and release personal information for the administration of common/shared programs and services. Examples of the various acts and regulations considered, on a program-by-program basis, include:

- *The Local Authority Freedom of Information and Protection of Privacy Act*,
- *Education Act*,
- *Statistics Canada Act*,
- *Canada Student Financial Assistance Act*,
- *Post-secondary Graduate Tax Credit Act*,
- *Skills Training Benefit Regulations*,
- *Post-secondary Education and Skills Training Act*,
- *Student Assistance and Student Aid Fund Act and Regulations*, and
- *Training Allowance Regulations*

9. Learning (continued)

The Provincial Examinations, Student and Teacher Services branch's personal information is governed by the *Education Act*, 1995 Part III - s 4 (1)(l), Powers of the Ministers to collect, the FOI Act – s 25, 26 (2) 27, 28, 29 (2)(e)(f)(k) and the Teacher Certification Regulations s 3(1)(a).

There are no other information requirements aside from legislation that affect Saskatchewan Learning Department's management of personal information.

With respect to student information in the Provincial Examinations, Student and Teacher Services branch, restricted access to an individual file can be applied in the event of a court order in child custody cases.

Release of information at the aggregate level is consistent with the Department's Education Indicators initiative. Every second year, the Department publishes an annual report on Education Indicators, which includes statistical information on things such as graduation rates, drop out rates, student demographics, student/teacher ratios, etc. Indicators are determined in extensive consultations across the Department as well as with education partners through the Evaluation and Monitoring Advisory Committee.

Overall, the provincial *FOI Act* governs the Department regarding the management of the personal information collected, used and released. However, additional, specific information requirements, such as, statements on how the information will be used, security, restrictions, liability, duration and termination, law of contract, and frequency and mode of data transfer, etc., are addressed in the respective Memorandums of Understanding and Data Sharing Agreements.

On a client-by-client basis, there are processes to manage specific personal information restrictions (e.g. restricting the production a particular client's transcript). Also, a restriction on who can view specific clients' addresses is currently in development as this is an issue with child custody cases.

ACCOUNTABILITY

The following individuals are accountable for managing the policies regarding personal information and overseeing compliance with them at Saskatchewan Learning. For the *Freedom of Information and Protection of Privacy Act*, the FOI Access Officer's mandate and role is stated. Executive Directors are responsible for all personal information under their control, which includes corporate and branch program policies. Director and Supervisors are accountable for personal information in their control and the branch's business processes and practices. Further description of end-user and branch responsibilities is addressed in the Department's *Information Security and IT Acceptable Use Manual: for end-users of Department, Information System*.

9. Learning (continued)

The Quality Assurance Services Unit has the authority to audit all aspects of income support programs in the Department. Quality Assurance review activities include, but are not limited to, examining if employees' actions are in compliance with policies, standards, procedures, applicable laws and regulations. Included also are compliance reviews to determine the adequacy of systems, practices, and controls in place to ensure compliance with relevant legislation, regulations, agreements, policies, etc. and to report on the extent of compliance.

The Director, Information Technology Services, is responsible for network accounts, user access and user accounts. The Manager of Corporate Information, Corporate Information and Technology, is responsible for corporate-wide information management, which includes business and information technology adherence to access and privacy regulatory functions (e.g. data requirements, data quality, *FOI*, and data sharing agreements). Upon public request, the identity of the above individuals is made known.

At the Provincial Examinations, Student and Teacher Services branch, the Registrar, Provincial Examinations, Student and Teacher Services administers policies related to credit requirements for secondary level completion, grade 12 department exams and maintenance of a central registry of Saskatchewan students from K-12.

The Assistant Registrar, Teacher Services and Certifying Official administers policies related to teacher certification and classification and manages a central registry of all teachers certified in the province. Upon public request, the identity of these two individuals is made known.

Saskatchewan Learning retains third parties to conduct program evaluations. As part of this process, certain personal information is provided to the third party where necessary, to enable them to contact clients to evaluate client satisfaction with services provided.

For purposes of the student loan program, Saskatchewan Learning works cooperatively with service providers, as follows:

- the Royal Bank and HRDC service providers for repayments and disbursement of student loans
- Credit checks with collection agencies
- Institutions and schools (SIAST, Regional Colleges, Community Based Organizations, Regional Offices) to collect personal information on behalf of the Provincial Training Allowance Program
- Canada Customs and Revenue Agency ("CCRA") for T slips submissions
- Canada Millennium Scholarship Foundation for verification and monitoring of applicants for student bursaries, as per agreement

9. Learning (continued)

- Department of Social Services for student loans and Provincial Training Allowance (PTA) to determine eligibility and to ensure no duplication of funding
- Department of Health for nominations of health benefits for PTA clients
- HRD Canada for approval, processing and collection of student loans

All MOUs and data processing agreements address confidentiality, privacy, and the treatment of personal information.

The Provincial Examinations, Student and Teacher Services branch does not outsource processing (IT or otherwise) of its personal information.

To protect the information in Saskatchewan Learning's care that is being used by third parties, the Department has standards for sharing information. All data processed by an external agency or department must be clearly defined within the context of the governing acts and regulations, with further conditions and restrictions stated in the respective Service Contracts, MOUs and Data Sharing Agreements. For example, upon termination or completion of a service contract the external agency is required to sanitize all hard drive(s) where the personal information resided.

In addition to *The FOI Act*, the Canadian Standards Association Model Code for the Protection of Personal Information is also referred to when developing practices that control the amount, use, and disclosure of personal information.

Saskatchewan Learning uses the following written policies or procedures with respect to personal information in their possession: *Information Security and IT Acceptable Use Manual* - for end-users of department, Information Systems, as well as other policies and procedures. When asked, the information is provided to the public, with the exception of the *Saskatchewan Post-Secondary Education and Skills Training Security Project: Information Technology Security Project* for technical security reasons.

Saskatchewan Learning has communicated its policies to all employees so that they are fully aware of their obligations. On a semi-annual basis (January and September) the Department's *Information Security and IT Acceptable Use Manual* is sent to all staff with an accompanying memorandum from the deputy minister. Executive Directors and Directors are also reminded to ensure this document is circulated to all their employees. This document is also filed in the Department's public directory.

9. Learning (continued)

Some but not all employees have received formal FOI training. The last FOI training sessions were held during 1993-94. Awareness regarding the protection of personal information is usually through new staff orientation and informal discussions with staff pertaining to a specific event.

Saskatchewan Learning has established procedures to receive and respond to complaints and inquiries. Program managers are the first line of contact. If the issue impacts more than one program area then resolution will be a joint effort. If necessary, the complaint or inquiry is escalated to the FOI access officer for resolution and guidance. Complaints addressed to the Privacy Commissioner's Office are directed to the FOI access officer for appropriate action and resolution.

The Provincial Examinations, Student and Teacher Services branch uses the Release of Transcripts Policy as written policy and procedures with respect to personal information in the branch's possession. This policy is available publicly and the branch does tell individuals about it when appropriate. For student information, the transcript release policy is posted at the front reception. For teachers, a statement of purpose for collecting appears on the application for certification and information is provided in response to inquiries.

The Student Information Transcript Release policy was last updated in June 2002 while the teacher information was updated in 2001. The Student Information policy is posted to communicate it to employees while the teacher information manual is supplied to all Teacher Services employees.

All employees are trained with respect to the protection of personal information. New employees are trained on an individual basis with ongoing supervision. The branch has also established procedures to receive and respond to complaints and inquiries. In both areas an inquiry line exists to respond to the public. For students, problems are referred to the Registrar. For teachers, problems are referred to the Certifying Official.

Information technology security and other policies and procedures are in place to protect personal information, such as, regular password control, secure systems, limited access to end-users by roles and responsibilities, and controlled processes.

9. Learning (continued)

Saskatchewan Learning uses the following to monitor compliance with the above procedures:

- To ensure the personal information is accurate and complete, daily and weekly data quality reports are generated, and distributed to respective business areas for correction (e.g. Data is outside of acceptable range, inconsistent with valid values, does not confirm to business rules, etc.).
- A data coordinator works on a daily basis with a defined group of key employees that represent all of the facets of the assigned business areas. This group is responsible for working with the data steward on a variety of tasks, such as, establishing data quality metrics, creating and maintaining record merging and archive rules, and enforcing data security rules within their business areas.
- Supervisors audit staff interactions with clients, review staff system access, and review audit trails on users accessing the system.
- IT monitoring of network security (e.g. firewall)
- When complaints are received, (i.e. become aware of non-compliance) steps are taken to correct and improve.

At the Provincial Examinations, Student and Teacher Services branch, in order to monitor compliance with the above policies and procedures, an audit function is built into both the Student Records System and the Teacher Records System.

Verification/check points are built into the processing procedures and through daily supervision of employees.

IDENTIFYING PURPOSES

To determine what personal information Saskatchewan Learning needs to collect and maintain, program managers, business area representatives, business analysts, information technology analysts, and a data architect arrive at consensus on what data is required to deliver a particular program/activity. Only required information is collected and maintained (“nice to know” information is not collected).

The information collected and maintained is for a purpose that relates to an existing or proposed program of Learning. For example, income support programs are dependent on the personal information received. Audits and validation processes are routinely conducted (i.e. need to ensure that the individual is who they claim to be and that they can be located).

9. Learning (continued)

To determine what student information the Provincial Examinations, Student and Teacher Services branch maintains, the branch needs supporting documentation to determine secondary level standing. The K-12 student tracking initiative is under development; consultations are underway with education partners (Saskatchewan Learning, school divisions, First Nations organizations).

To determine what teacher information the branch needs to collect and maintain, the branch needs supporting documentation to identify the individual and qualifications to warrant certification. There is ongoing information sharing with universities and other provincial ministries of education.

Saskatchewan Learning does not identify the types of personal information that it collects and does not classify the information according to its sensitivity. Currently all personal information is classified as sensitive. The Department classifies employees in accordance with their duties and responsibilities as to the degree or level of access to personal information. User level security is based on roles and responsibilities of the work required/job requirements.

Locked doors, locked program areas, locked cabinets, locked file rooms and security pass cards are used as physical security measures. Controlled passwords and firewalls are also used.

Executive Directors and Directors are responsible for the respective program areas that use personal information. Examples of officials with this role are as follows:

- Director of Assessment, Income Support Programs (paper)
- Manager of Business Information and Technology Services, Income Support Programs (electronic)
- Director, Loan Management and Financial Services (PTA paper files)
- Director, EAPD, Literacy, ESL, Program Agreements, and GED

For Information Technology:

- Director, Corporate Information and Technology
- Director, Technical Services (user ids and passwords)
- Application Architect
- Director of Maintenance

The Provincial Examinations, Student and Teacher Services branch identifies and classifies teacher information they collect. For teacher information, different users require different information. The purpose of the receiving agencies must be consistent with the purpose for which the information was collected.

9. Learning (continued)

While student information is not defined in written policy in this manner, in practice the information is classified as public at the aggregate level and restricted at the personal level. Teacher information is classified as public, restricted professional and restricted personal.

The most sensitive information is housed as follows: Prior to approximately 1930, student information was housed in provincial archives. From 1930-1972, the information was stored in cardex files in a locked file room on site. From 1972 to present, the information is stored on a Unix platform with an Ingres operating system.

For Teacher information, paper records are housed in a locked file room on site although some early records prior to 1970 are on microfiche on site. Information in electronic files is stored in Unix with an Oracle operating system developed in 1995.

Saskatchewan Learning creates personal profiles by combining personal information from various sources. Sharing of information across program areas is specific to the delivery of the program.

Specific employees have access to personal information from various sources. Their access is based on the work/job duties that must be performed to fulfill the mandate of delivering a particular program(s).

As a result of policy, programs, and organization changes, 'what is required information' is under routine review. Information received from external agencies is generally verified through direct consultation with the client or through audit practices.

Saskatchewan Learning tells individuals in advance why their personal information is being collected and how it is going to be used. Client declaration/ consent forms are included in all application forms and are vetted through Justice.

The Provincial Examinations, Student and Teacher Services branch also tells individuals in advance why their personal information is being collected and how it is going to be used. Student information is collected from the schools (a statement appears on the scannable form as well as in the Registrar's Handbook for School Administrators which is available online). As work proceeds on the K-12 student tracking project these statements will change. There is a concern about the number of children who are not registered in school, or who are

9. Learning (continued)

registered but not attending. In order to intervene appropriately the province needs a system to track students. The new K-12 student tracking system will enable the Department to monitor retention rates, completion rates, progress and movement of students. For teacher information, teachers complete a statement on the Certification Application Form and the annual Educator Profile Form.

Saskatchewan Learning assesses personal information-related risks prior to implementing a new business process reliant on the collection and use of personal information. Risks are identified when developing new business requirements. New business processes are required to follow the same strict regulations governing branch operations. New business processes and regulations are constantly evolving in conjunction with the ever-changing availability of new ways to deliver programs and services to clients (i.e., ever-changing technology).

The Provincial Examinations, Student and Teacher Services branch assesses personal information-related risks prior to implementing a new business process reliant on the collection and use of personal information. Consultation is made with Justice, the STF, SSTA, School Divisions and other provincial ministries of education.

When implementing a new technology or system, privacy concerns are addressed by developing business and technical processes and solutions. These generally involve business representatives from the program area(s), a data architect, manager of corporate information, application architect, project manager, lead IT developer, provincial auditors and controllers, and Justice. Privacy is always considered in the development of new processes or systems.

Processes assisting in addressing privacy concerns at the Provincial Examinations, Student and Teacher Services branch, include processes such as the “Student Tracking Project – Security Access Authorization” agreement and “Student Tracking Protocol”, which must be agreed to and followed by users of the new student tracking system. The authorization agreement and protocol clearly inform the user (school principal, vice-principal, director of education, etc.) of Learning’s authority to collect information, the purpose for which the information is being collected, the confidential nature of the information and how it is to be used.

Individuals who collect personal information from students and teachers are trained on how to describe what the information is going to be used for. Training is provided to new staff members who deal with the public. When students or teachers are concerned about providing information, staff can provide a copy of the declarations that they had previously signed. Full disclosure and counseling is available for individuals concerned about providing information.

9. Learning (continued)

At the Provincial Examinations, Student and Teacher Services branch, employees are made aware of the purpose for collecting the information and are able to communicate this to students and teachers. Regarding teachers specifically, the annual Educator Profile, which they must complete, expressly states at the beginning of the form the purposes for which the information is collected.

CONSENT

It is Saskatchewan Learning's policy to gain consent from individuals for the collection and use of their personal information. Client declaration/consent forms are required, which includes the client's signature. All forms are included with client program/service applications. These forms must be signed before the application can be processed through to completion.

At the Provincial Examinations, Student and Teacher Services branch, student information is received from a third party. Information is provided by a student/parent when the student enrolls in a school.

For the K-12 student tracking project Learning observes it may not be reasonable to seek consent nor always possible given that the project is designed to identify students not registered or not attending school. Learning advises that these issues will be discussed as the student tracking project proceeds.

For teacher information, teachers provide consent by completing a statement on the Certification Application Form (signature) and the annual Educator Profile Form.

Consent is recorded through both paper and electronic formats. For paper record, the consent form is signed by the client and stored by the specific program business area. For electronic record, the signature date of the consent is entered on the system.

At the Provincial Examinations, Student and Teacher Services branch, student information consent is recorded at the school level in the Student Records System. Pursuant to the Education Act, all children between 7 and 16 must attend school. Consent is recorded for teacher information as a signature on the original Application for Certification Form and Confidential Disclosure document.

With client consent stored electronically and on paper, it is shared with those employees who require this information, which ensures that users of the information know consent has been obtained.

9. Learning (continued)

At the Provincial Examinations, Student and Teacher Services branch, users of personal information up to this point in time have been department employees only and they are aware of how consent is obtained and the purpose for which the information was obtained. However, the expansion of the student tracking system during the upcoming school year and implementation of online student tracking will add third party users to the system (i.e., school principals, vice-principals, directors of education and/or their support staff). Protocols regarding the management of this information have been developed and have been reviewed with the Department of Justice.

The “Draft Student Tracking Protocol” statement deals with the type of information to be gathered, the use of the information and the sharing of the information. Learning, FSIN, and school boards have all agreed to the draft protocol.

For teacher information, all users within the Unit have access to Learning’s policy manual, which deals with consent and the use of personal information.

Saskatchewan Learning uses the following techniques to ensure that the personal information use is only in accordance with the consent obtained:

- Security levels are granted to employees according to the duties to be performed.
- Employees are to gain access only to information required to perform their job duties, which are routinely reviewed by program managers and the data quality committee.
- Program managers and IT are informed as to the conditions specified in the memorandums of understanding and program data sharing agreements to ensure that personal data is collected, used and released as intended and as consented to by the clients.
- Provincial auditors, controllers and supervisory monitoring of staff are also used.
- For Quality Assurance, daily checks are made to ensure that the client’s data collected is tied to a program or service. As well, routine data quality reports are generated to determine if the information is complete, accurate, and timely.

At the Provincial Examinations, Student and Teacher Services branch, in order to ensure that the personal information’s use is only in accordance with the consent obtained, an audit function built into both the Student Records System and the Teacher Records System performs verification/check points, which are built into the processing procedures. The daily supervision of employees also helps to

9. Learning (continued)

control the use of personal information. Unusual requests for information require authorization of the Registrar for Student Records System and Certifying Official for Teacher Records System. An example of an unusual request for student records would be in an instance where the legal guardian of a dependent adult requests information for a student that has become incapacitated. An example of an unusual request for teacher information could be a situation where descendant of a deceased teacher is requesting information about the teacher for compiling a family history.

Saskatchewan Learning informs individuals and gains their consent prior to disclosing their personal information to any third party. At the onset, through the client declaration/consent process, clients requesting programs/services are informed as to the purpose for collecting the information, how it will be used, and to what department or agency it will be released.

If Saskatchewan Learning wants to use the personal information for a purpose not previously identified, consent is regained. Information is used only for the purposes for which it was originally collected. Instances where the Department regains consent is, for example, if a Bank sends a signed client consent to release personal information to the particular Bank requesting this information or where advocates of the disabled, who conduct hearings on behalf of disabled clients, require information. In these cases, Learning requires written permission from the student or client requesting personal information in its possession to be released to the Advocate.

At the Provincial Examinations, Student and Teacher Services branch, the information is used in the ways identified and is generally not shared.

LIMITING COLLECTION

In order to ensure that Saskatchewan Learning only asks for personal information that they need to use, the process used is one of consensus by all involved in the collection of personal information (Business area and IT with guidance from Justice). Privacy concerns are addressed during the development of business and technical processes and solutions. This process generally involves the program business representatives, data architect, manager of corporate information, application architect, project manager, lead IT developer, and provincial auditors and controllers.

In the event that additional information is required from an outside agency or department, the requesting program area must submit the rationale to corporate information management. In turn, the source agency or department is contacted

9. Learning (continued)

and if agreed to, amendments are made to existing MOUs or data sharing agreement. Requests for additional, required information is completed and approved by the business area executive director, corporate manager of information, and the source.

At the Provincial Examinations, Student and Teacher Services branch, in order to ensure that the branch only asks for personal information that they need to use, requests are consistent with legislated requirements. As well, information is used at the aggregate level to support the Education Indicators Program as previously discussed and also supports legal obligations for submitting information to Stats Canada.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

To ensure that personal information is only used for the purpose for which it was originally collected, all information entering and leaving the Department's database requires an MOU or data sharing agreement. Program managers and staff are responsible for day-to-day operations, which includes training and staff audits. The level of security granted to each employee is the branch responsibility and requires branch approval.

In order to ensure that personal information is only used for the purpose for which it was originally collected at the Provincial Examinations, Student and Teacher Services branch, user authorization is required on both systems and users are guided by policy.

Saskatchewan Learning uses *The Saskatchewan Archive Act* as a formal policy in place with respect of the retention and destruction of personal information. More specifically, the Provincial Examinations, Student and Teacher Services branch uses the Records Retention and Disposal Recommendations of *The Saskatchewan Archives Act* s 8, which requires that student and teacher records be permanently retained.

Saskatchewan Learning does destroy, erase or anonymize personal information that is no longer in use in accordance with the Saskatchewan Archives, which is the only body that grants permission to destroy personal information. Copies of personal information (e.g. paper hard copies) that are no longer required are to be shredded by the respective program business areas. In the event of personal data, in electronic format, copied from 'old' hardware to 'new', the 'old' hardware is sanitized (i.e. overwritten by a software package) prior to the hardware being recycled/reclaimed.

9. Learning (continued)

Saskatchewan Learning collects personal information about an individual from third parties. When shared responsibility for program delivery with other departments and institutions exists, personal information may be collected from others such as:

- Student Financial Assistance: parents and spouse information
- Apprenticeship and Trade Certification Commission: employers
- Credit reporting agencies
- Regional Services
- CCRA
- Financial Service Providers
- Royal Bank
- Lawyers
- Social Services
- Maintenance Enforcement (Justice)
- Anonymous callers to Audit Unit
- HRDC (restrictions)
- MOUs re: SAR, EI
- SGI
- Graduate Tax Credit (FOI, 26(1)(e)(a)(b))
- Education/Training institutions

The Provincial Examinations, Student and Teacher Services branch also collects personal information about an individual from individuals other than him or her. Student information is collected from schools and school boards. Teacher information is collected from school boards, universities, other provincial and state education officials, teacher exchange officials and disciplinary information is collected from the STF.

MAINTAINING ACCURACY

Saskatchewan Learning does ensure that the personal information that they collect, use and disclose is accurate, complete and up-to-date. They do so through the following:

- regular audits
- verification with the client/third party
- weekly data quality meetings with all program business area representatives, data quality coordinator, director of maintenance, and manager of corporate information
- constraints in database design
- edit checks
- measures mentioned in the “Consent” and “Accountability” sections

9. Learning (continued)

The Provincial Examinations, Student and Teacher Services branch ensures that the personal information that they collect, use and disclose is accurate, complete and up-to-date. Reports regarding student information are sent to schools for verification twice per year. This will change with the K-12 student tracking project (enrolment and withdrawal changes will be submitted online as they occur). For teacher information, official and up to date transcripts are required for the initial assessment to create the teachers file. Ongoing teacher assignment information is entered from the Education Profile submitted by the teacher on an annual basis with verification at the school level.

SAFEGUARDS

Saskatchewan Learning has various safeguards in place to protect personal information from unauthorized access, disclosure, copying, use or modification. Secured areas for paper files and server rooms, tracking system for paper files, secured electronic and physical access (e.g. password controlled, user level security, employee access cards), firewalls, encryption for file transfers, and secured file transfer servers are all methods used by Learning.

Physical measures in place to protect personal information include employee card access, locked cabinets, locked offices, desk top log off, secured access doors, security patrolled during off hours, and locked server rooms with limited access among IT staff.

Organizational methods used to protect information include limited access on a need to know basis, which is dependent on an employee's role and responsibilities specific to a particular program or service. Technologically, Saskatchewan Learning uses user passwords, encryption outside the firewall, secure file transfer servers, strict data sharing protocols that every agency or department has to follow (i.e. Learning's standards are not relaxed because a third party cannot adapt), user level of security and firewalls.

The Provincial Examinations, Student and Teacher Services branch also has safeguards in place to protect personal information from unauthorized access, disclosure, copying, use or modification. For both student and teacher information, paper files are housed in locked file rooms and electronic files require authorization with varying levels of access existing. Along with the locked file rooms, the work area is restricted to the public as a form of physical restriction. System users have different levels of access on the system and access is limited to 'need to know'. Technologically, the branch uses passwords, firewalls and encryption to protect the information.

9. Learning (continued)

Saskatchewan Learning employees, contractors, partners and any other third parties with whom personal information is shared are normally required to sign confidentiality agreements. Employees are required to sign an *Oath or Declaration of Office* when they are hired. Contractors must sign a Consulting Services Contract. Third parties must sign either a contract or an agreement with each of the service providers, in the form of a Data Sharing MOU or of a Data Sharing Agreement.

At the Provincial Examinations, Student and Teacher Services branch, in some cases but not all information regarding students may be shared with school principals without the principal signing a confidentiality agreement. The *Education Act* provides for the sharing of information between schools and the Department. In order to protect the information requested by a school principal, Learning will only provide student information to a principal by fax and Learning knows the fax numbers of all the schools in the province and the names of all the principals.

Student information is shared with schools and school boards without a signature. For teacher information, Saskatchewan Learning, the Teachers' Retirement Plan and the Teachers' Superannuation Commission have signed a memorandum of understanding. Information is shared with universities and other ministries of education without a similar process.

Saskatchewan Learning has taken initiatives with the ITO or others to improve privacy and security. The ITO initiated a security charter for government that was endorsed by the Deputy Minister Steering Committee in December 1999. As a result of that, the Department undertook the development of a departmental security policy. EDS was contracted to assist in this work and the security policy was completed by December 2000. CIT then took the policy to various steering committees, including the Department's Union Management Committee for feedback. The revised policy was shared with Senior Management and approved in the fall of 2001. The policy was formally introduced to all employees in the Department in the spring of 2002.

OPENNESS

Saskatchewan Learning communicates their policies, procedures, contacts, etc. regarding personal information to those who request it or the general public as follows. Between the Department and the general public, including other departments and agencies, primary communication is through the application packages and references are commonly made to Client Consent/Declarations, Mandate/description of program or service, *FOI*, Data Sharing Agreements,

9. Learning (continued)

and/or MOUs. The method of communication used is also dependent on the type of question(s) raised by the general public (e.g. phone, email, letter correspondence, department web site, referral to Program Manager, referral to FOI access officer for guidance).

At the Provincial Examinations, Student and Teacher Services branch, for student information, the Release of Transcript Policy is posted in the reception area for the public to view. A transcript request form is available on the web site. For teacher information, certification procedures are available on the web site and printed information is available upon request. Written and verbal explanations are provided on a regular basis for both areas.

PROVIDING ACCESS

Saskatchewan Learning allows individuals access to their personal information through personal requests and *The FOI Act* requests. As well, for teacher information, access is required under s 10 in the Provincial Collective Bargaining Agreement.

In order to release the personal information, Saskatchewan Learning needs to verify that the person requesting the information is the same person to whom the information is in reference to. Routinely, any type of assessment, repayment and verification information is released. General inquiries are handled by trained front line staff and may be escalated to particular supervisor/managers. The release of personal information is handled through mail, phone and in person. If the authority to release the personal information is unclear the FOI officer or Supervisor/Manager provides advice to Saskatchewan Learning.

At the Provincial Examinations, Student and Teacher Services branch, student information such as transcripts are mailed to students, schools and post-secondary institutions while teacher information such as certification status is routinely released to school boards.

The releasing of student information is the shared responsibility for a staff of 13 while the release of teacher information is the shared responsibility for a staff of 7. In order to release student information, staff follows Learning's transcript release policy. For mail requests in particular policy dictates that a mailed response can only be sent to the student at the student's mailing address currently on file with Learning. If the recipient requests that the information be sent to another address, Learning requires that the student provide Learning with a written authorized change of address request before any information will be sent to that address. Students can request that transcript information be sent directly to a post-secondary institution. In such instances Learning maintains a

9. Learning (continued)

mailing list of institutions and contact people at those institutions and Learning will only send information to a person on their listing. Students can also request information be sent to employers. Learning maintains a list of large corporate employers and Learning will only send information to employer Human Resource departments that are known to Learning and are on their mailing list. If a student requests that the information be sent to an unknown employer Learning will contact the student to make alternate arrangements for the release of the information.

For teacher information, if the recipient is a walk in, the release requires personal identification. As well, written permission of individual and payment of fees (signature verified against the file) is also required. If it is unclear if the information should be released, the branch receives advice from the following individuals:

- For student information, the Registrar is contacted first, then the Legal Officer, then Justice
- For teacher information, the Certifying Officer is contacted first, then Legal Officer, and then Justice

Saskatchewan Learning and the Provincial Examinations, Student and Teacher Services branch both record the information released, the name of the recipient and the date released.

Saskatchewan Learning and the Provincial Examinations, Student and Teacher Services branch both ensure that the released information is provided for under the “consent” and “identifying purpose” sections and that written confirmation is received prior to the release of personal information to a third party.

The recipient of the information is not necessarily contractually bound through agreements or otherwise to adhere with Saskatchewan Learning’s privacy policies. This would be the case where the recipient is a student, teacher, employer, etc.

At the Provincial Examinations, Student and Teacher Services branch, the recipient is contractually bound through agreements or is requested to adhere with the branch’s privacy policies. In most cases, Local Authority FOI and FOI legislation would govern the transaction. In cases outside the legislation a memorandum of understanding might be required or a User ID Assignment Form.

Saskatchewan Learning does delete, update or add to, an individual’s personal information where it is shown to be inaccurate, incomplete or out-of-date. An audit log is maintained of all changes made to a client’s personal information.

9. Learning (continued)

Saskatchewan Learning uses corporate audit to perform quality assurance reviews on data as well as information shared under MOUs and other agreements. Data quality reports are reviewed and Learning may contact the client to verify the information being reported.

Saskatchewan Learning does not obtain the consent in all cases of the person to whom the information relates before making any amendments. However, if the information is received from a source other than the client, the changes are verified with the client as required or are sent to audit for verification.

If the change(s) impacts a client's reassessment the client is advised. The information provided by the client is considered to be true and accurate (i.e. signed declaration). The signed consent/declaration provides the agreement from the client to verify and audit their entitlements for student financial assistance.

The Provincial Examinations, Student and Teacher Services branch also deletes, updates or adds to, an individual's personal information where it is shown to be inaccurate, incomplete or out-of-date. To confirm the amended information, the branch requires official documentation of name change, transcripts etc. For student information, consent is not obtained before making amendments. The information is verified at the school level. The teacher's consent is obtained before making amendments.

CHALLENGING COMPLIANCE

Saskatchewan Learning does have a formal process in place to deal with complaints about its personal information management practices or policies. Program managers are the first line of contact. When a program manager receives a complaint, it is evaluated within the context of existing business practices, and changes to the application and/or business practice may be required. If the issue impacts more than one program area then resolution will be a joint effort. If necessary the complaint or inquiry is escalated to the FOI access officer for resolution and guidance. Complaints addressed to the Privacy Commissioner's Office are directed to the FOI Access Officer for appropriate action and resolution.

The Provincial Examinations, Student and Teacher Services branch does have a formal process in place to deal with complaints about its personal information management practices or policies. Complaints are referred to the Registrar (legal advice would be sought from Legislative Services within the Department and the Department of Justice).

9. Learning (continued)

Saskatchewan Learning reports receiving two complaints as follows, regarding its personal information management practices over the last twelve months. The privacy commissioner was contacted on 2 separate occasions regarding:

- The accuracy and completeness of personal information
- Justification for asking for specific personal information

The Provincial Examinations, Student and Teacher Services branch reports one breach of the policy and procedures pertaining to the handling of personal information in the past 24 months as follows. The issue is in respect to the student system, wherein an individual is currently pressing charges against a second individual for allegedly obtaining the first individual's academic record fraudulently. The action taken by the unit was to tighten up the requirement for verifying the identity of an individual when purchasing a transcript.

RECOMMENDATIONS

1. Learning should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. Learning should establish formal accountability for privacy within the Department.
3. Learning should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
4. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.
5. We recommend that Learning consider using the government's data classification scheme (to be developed) to confirm the sensitivity of the information under its care. Policies should be reviewed to determine the appropriate levels of safeguard for the information held.
6. Learning should implement consistent policies and procedures, which would require that all employees, contractors, partners, or other third parties with whom personal information is shared be required to sign confidentiality agreements.
7. Learning should continue to incorporate informed consent into new processes and programs.

9. Learning (continued)

8. Learning should consider implementing those information security recommendations of the Provincial Auditor not yet implemented to provide enhanced safeguards to personal information.
9. Learning should continue to conduct reviews, including compliance with *FOI* processes and safeguard audits (e.g. technology).
10. Learning should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this overarching policy, each Branch should review its current policy to ensure alignment with departmental policy.
11. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

10. SaskEnergy

INTRODUCTION

SaskEnergy Incorporated gathers information to ensure and determine customer identification for billing purposes. SaskEnergy collects customer name, current and previous address. They also request that at least one of the following be provided as an identifier: Saskatchewan Health Services Number, driver's license, or date of birth. If applicable and offered, a treaty number will also be accepted. Social Insurance Numbers are not requested, however, SaskEnergy will accept it, if offered by the customer.

SaskEnergy does not collect information on behalf of another department, agency or level of government. All information that is collected is for SaskEnergy's use.

SaskEnergy shares personal information regarding collection of debts, billing, and other direct customer contacts with other groups or sections within the organization. In addition SaskEnergy shares personal information with other Crowns, government agencies such as Social Services, and municipal governments for payment of accounts, collection of debts or verification of information. They also receive personal information from these entities for the collection of debts or verification of information.

SaskEnergy determines what is personal information as per SaskEnergy's Code of Conduct. All customer personal information collected at SaskEnergy Incorporated is classified as confidential.

The Freedom of Information and Protection of Privacy Act and *The SaskEnergy Act* govern SaskEnergy's use of personal information. Aside from this, SaskEnergy has participated in establishing the government Security Charter on computer security, which also affects the management of personal information.

ACCOUNTABILITY

At SaskEnergy, the following individuals are responsible for managing the policies regarding personal information and overseeing compliance with them. The General Counsel and Corporate Secretary, who is also the FOI Access Officer, is responsible for the approval of the release of information. The Vice President of Information Systems is responsible for computer-related policies. The Manager of Business Policies is responsible for the development and implementation of customer business policy regarding personal information. The names of these individuals are made known to the public upon request.

SaskEnergy does outsource some of its handling of personal information. The SaskEnergy Customer Billing system runs on a mainframe at ISM and energy bills are printed, stuffed and mailed there as well (along with SaskPower's).

10. SaskEnergy (continued)

SaskEnergy also has ISM and other contract programmers supporting and enhancing the billing system. ISM staff and sub-contractors sign a confidentiality agreement with SaskEnergy, in order to protect the personal information in their care.

SaskEnergy's Code of Conduct policy is used for written policies or procedures with respect to personal information in SaskEnergy's possession. This policy, which was last updated May 9, 2000, is available to all employees and would be provided upon request to third party individuals. In order to ensure that SaskEnergy has communicated this policy to all employees so that they are fully aware of their obligations, all employees have been advised of the Code of Conduct policy through e-mail advisory. Ongoing awareness sessions are held throughout the corporation, where the topic of confidentiality is regularly discussed in order to protect personal information. In order to deal with complaints or inquiries, as a standard business practice, any complaints or inquiries are forwarded to the department responsible.

Currently in place, SaskEnergy uses the Code of Conduct policy, Information Systems Data Related policies and Access Control policies to protect personal information. Compliance with the Code of Conduct and Access Control policies is monitored by following up on complaints from customers. For Information Systems policies, SaskEnergy uses a combination of access reviews for detective and corrective controls to monitor compliance with the policies.

IDENTIFYING PURPOSES

At SaskEnergy the billing system requires certain information fields to be completed in order to have enough information to provide a bill and to ensure that the proper person is listed on the account. This information requirement determines what personal information SaskEnergy maintains.

As per the Code of Conduct, all personal information is considered confidential. SaskEnergy does not go any further to identify the types of personal information that it collects nor to classify that information according to its sensitivity. Information that SaskEnergy considers sensitive (confidential), is stored on the mainframe, LAN/WAN, Oracle databases on disk and on backup media, paper and CD. The VP Information Systems is responsible for the area that manages the above media.

SaskEnergy creates personal profiles by combining personal information from various sources. For billing purposes, customers are grouped together based on a variety of determiners, such as location, usage, and type.

10. SaskEnergy (continued)

SaskEnergy verbally tells individuals in advance why their personal information is being collected and how it is going to be used. At the time the customer contacts SaskEnergy for service connection, either over the phone or in person, it is explained that SaskEnergy requires the information for billing and verification purposes. Because applications are accepted over the telephone, identifiers known only to the customer must be provided to SaskEnergy.

Prior to implementing a new business process reliant on the collection and use of personal information, SaskEnergy does assess personal information-related risks. When purchasing new software or developing software, Information Systems works with the business unit to determine who should have access to the system and data. SaskEnergy establishes suitable security profiles and assigns these to those individuals who require access. When an employee changes jobs, the system access is transferred to the new employee filling the position. For changes to business processes, Information Systems assesses risk to personal information through risk management processes.

When a new technology or system is implemented, SaskEnergy incorporates the protection of personal information by treating a new technology just like other new systems. In recent years, SaskEnergy has moved into Internet applications to serve external customers. SaskEnergy worked with their legal department to determine what information would be available to customers. User access is controlled by user-id and password. For some applications like entering a meter read, SaskEnergy only requires an account number and meter number to accept a reading. SaskEnergy does not divulge any personal information in these applications. If SaskEnergy allows customers to view or update personal information, they will utilize user ids and passwords.

It is standard business practice at SaskEnergy to explain why they are requesting the information.

CONSENT

At SaskEnergy, in order for a customer to receive natural gas service they must provide the required information. SaskEnergy staff tell customers why the information is being gathered and how it will be used. Consent is, therefore, gained by their provision of the information. For any other reason, SaskEnergy would require the customer's signed agreement to collect information, such as a credit check.

The consent is recorded either electronically or on a prepared form related to the request. Provision of the consent in either format must be provided to users of the personal information to inform them that specific consent has been obtained.

10. SaskEnergy (continued)

SaskEnergy monitors by complaint to ensure that the information is used only for the purpose of the consent obtained. If SaskEnergy wants to use the personal information for a purpose not previously identified they regain consent from the individual. A typical example of this would be a real estate agent requesting consumption information for a particular residence. In such an instance SaskEnergy requires written consent from the customer.

LIMITING COLLECTION

SaskEnergy billing system requirements allow a limited amount of information to be input, which ensures that SaskEnergy only asks for personal information they intend to use.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

The SaskEnergy Code of Conduct requires that personal information only be used for the purpose for which it was originally collected.

SaskEnergy uses SaskEnergy's Information Asset Protection Program as formal policy guidance for the retention of personal information. The Program includes backup and retention standards for each platform where personal customer information is stored. With respect to the destruction of information, standards for the safe destruction of data are included within the Program. SaskEnergy does not destroy, erase or anonymize personal information that is no longer in use. ISM through the facility management agreement with SaskEnergy, destroys or erases personal information stored on mainframe backups, according to a pre-defined schedule.

SaskEnergy collects information about an individual from third parties for collection of debt or extension of credit (credit check) purposes.

MAINTAINING ACCURACY

SaskEnergy does not have formal procedures in place to ensure that personal information that it collects, uses and discloses is accurate, complete and up-to-date. If a customer's personal information is inaccurate, SaskEnergy's billing and collection process will generally detect this. Information is collected when customer connects and is not updated on a regular basis. If the customer contacts SaskEnergy at anytime the system information is checked and updated at that time if required. SaskEnergy, therefore, does not make outbound calls for purpose of updating information.

10. SaskEnergy (continued)

SAFEGUARDS

SaskEnergy does have safeguards in place to protect personal information from unauthorized access, disclosure, copying, use or modification. SaskEnergy's Code of Conduct, Access Control Policy and non-discretionary controls such as passwords and limited computer access all are safeguards that are used. Locked file rooms, key card access to offices and access to system limited to authorized users are physical measures in place to protect personal information.

Limited access to information restricted to authorized users is an organizational method used to protect personal information. Technologically, SaskEnergy uses access controls such as passwords, firewalls, encryption, auditing features and logs, as well as card-access systems for physical access controls to protect information.

Employees, contractors, partners and any other third parties with whom personal information is shared are required to sign confidentiality agreements. Contractors and partners or their firms on behalf of their employees sign the confidentiality agreements.

In order to improve privacy and security, SaskEnergy has participated fully with the ITO to develop a framework for use by other government agencies and crown corporations. As well, Information Systems policies have been completely rewritten within the previous two years.

OPENNESS

Communicating SaskEnergy policies, procedures, contacts, etc. regarding personal information to those who request is done so verbally, either in person or over the telephone. Written or faxed requests may be responded to in like fashion. Information Systems policies are shared corporate-wide on a Lotus-Notes bulletin board.

PROVIDING ACCESS

SaskEnergy does allow individuals access to their personal information upon confirmation of their identity. The process to release the information is as follows: If customers request their own information SaskEnergy requires a validation of the information on the system (Health Card number, driver's license number, etc.) to confirm identity. Information released is typically limited to the confirmation of a customer's address.

Unless exempted under the *Freedom of Information and Protection of Privacy Act*, all third party requests must be accompanied by the written permission of the customer to release the information to the requestor. Routinely, verification

10. SaskEnergy (continued)

of the customer's residence and annual amount of natural gas consumed at that location is released to third parties such as real estate agents once customer consent is obtained. Requests or inquiries for information may be received and handled by any of the authorized system users. Where information is released to third parties, SaskEnergy will also provide this information to the customer if they request it.

With respect to handling the release of personal information, information is released to third parties by regular mail, fax, e-mail or picked up in person, depending on who is requesting the information. Government agencies such as Social Services, Crown Corporations or Municipal Governments who are requesting the information for verification of customer information or the collection of a debt may be provided the information over the telephone, in very rare circumstances, if the SaskEnergy employee is sure that the requestor is authorized to receive this information. Normally SaskEnergy would receive a written request for information and would provide a written response. In rare circumstances SaskEnergy may receive a verbal telephone request for information, which is normally a request to confirm a customer's address, and if the SaskEnergy employee has a business relationship with the requestor and is very certain about the identity of the requestor they will release the information. In most instances, the type of information that would be released over the phone would be the confirmation of a customer's address. SaskEnergy's legal department advises SaskEnergy if the authority to release the personal information is unclear.

SaskEnergy records the information released, the name of the recipient and the date released except for information provided over the telephone to Government agencies, Crowns or Municipal Governments, which may not be recorded. As previously noted, the provision of information over the phone reportedly is quite infrequent and the information released is limited to the confirmation of a customer's address.

SaskEnergy ensures that that the released information is provided for under the "consent" and "identifying purpose" sections. SaskEnergy strictly adheres to procedures set out in the *Freedom of Information and Protection of Privacy Act*.

The recipient of the information is not contractually bound through agreements or otherwise to adhere with the department or agencies privacy policies. Information released over e-mail carry a disclaimer to advise that the information is meant for the person indicated and that legal action will be taken if unauthorized use of the information occurs.

10. SaskEnergy (continued)

SaskEnergy does delete, update or add to, an individual's personal information where it is shown to be inaccurate, incomplete or out-of-date. This is done through quality assurance programs or when customers advise SaskEnergy. The information is confirmed with the individual affected. Consent is obtained from the person to whom the information relates before any amendments are made.

CHALLENGING COMPLIANCE

SaskEnergy does have a formal process in place to deal with complaints about its personal information management practices or policies. Complaints received are passed on to the respective department head for action. SaskEnergy reports it has not received complaints regarding its personal information management practices over the last twelve months and has not experienced any breaches of the policies and procedures pertaining to the handling of personal information in the past 24 months. While there have been no reported breaches of confidentiality, SaskEnergy has recently developed comprehensive policies and procedures to support the release of information to third parties.

RECOMMENDATIONS

1. SaskEnergy should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. SaskEnergy should establish formal accountability for privacy within the Crown Corporation.
3. SaskEnergy should evaluate the overall privacy framework of the Government of Saskatchewan to be developed and assess whether or not additional policies and procedures need to be implemented to support the framework.
4. In the development of contracts with outside parties, SaskEnergy should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Corporation provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Corporation's personal information (privacy) requirements.
5. SaskEnergy should implement a formal system for the identification of the type of personal information it collects and the classification of the information as to sensitivity to determine the appropriate levels of safeguard for such information. SaskEnergy should ensure that this data classification scheme is compatible with the Government's processes (to be developed).

10. SaskEnergy (continued)

6. SaskEnergy should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed.
7. SaskEnergy should implement regular reviews to ensure compliance with FOI and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology audits).
8. SaskEnergy should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Corporation. This policy needs to balance the requirements identified in current policy with privacy considerations.
9. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

11. SaskPower

INTRODUCTION

In order to supply energy to individuals and to bill and collect for the energy provided, SaskPower needs to collect and use personal information. The data collected may include all or a subset of the following, depending on the customer circumstances:

- Name
- Address
- Phone numbers
- Names and phone number of contact people, which can be reached if contact cannot be made with the customer
- Employer (purpose of collecting this information is to assess credit worthiness and for contact information)
- Proof of identification
- Bank account information including bank account number, bank identification code, bank transit number and effective date person signed application for direct payment plan

The requirement to disconnect service is the final step if SaskPower cannot achieve payment arrangements. This often results in SaskPower discussing credit rating, collection actions undertaken, payments made by customers, etc. with outside agencies such as the Ombudsman's Office and Social Services. In addition personal information may be shared with SaskHousing, the Minister's Office, SaskEnergy, SaskTel, the RCMP, Sheriff's Office, Department of Justice and municipal police forces. These organizations will also share personal information with SaskPower.

SaskPower does not have a formal written guideline or policy that is used to determine what is personal information. The informal rule is any data stored in SaskPower's Customer Information (and Billing) System is considered personal. Any customer data contained in a contract with a key or major customer would be considered confidential information.

The *Freedom of Information and Protection of Privacy Act* governs SaskPower in respect of personal information. In addition legal or court order requirements may affect SaskPower's management of personal information.

ACCOUNTABILITY

SaskPower's Vice-President of Customer Services oversees the development and updating of policy and practice related to personal information. All Customer Services Managers are responsible for overseeing the implementation of policy. Customer Services Supervisors are responsible for implementing policy as it affects their area of responsibility.

11. SaskPower (continued)

The Supervisor, Business Policy in Customer Services is an advisor to all Customer Services managers and supervisors in interpreting policy, if required. All front-line staff are responsible for adhering to policy and practice.

SaskPower is currently developing a formal privacy program. The Chief Information Officer is responsible for the project. The program will determine the roles and responsibilities of the SaskPower privacy officer.

Currently SaskPower has a number of written policies and procedures with respect to personal information including the following:

- Release of Employee/Business Information Policy (September 2000)
- Code of Conduct (January 2001)
- Confidentiality Agreement (July 1999)
- Employee Personal Information Change Request (September 2001)
- ITM and Security Policy (January 1999)
- Customer Services Directive 93-03 (1993)

SaskPower does make its policies and procedures regarding personal information available to the public. SaskPower staff are able to access policies through SaskPower's Intranet and the Business Administration manual which contains all of the policies.

SaskPower has not provided formal training to its staff regarding the protection of personal information. SaskPower has identified this as a priority concern and hopes to have a formal training program in place in 2003. In May and June 2002 Customer Services front-line employees were sent e-mails clarifying SaskPower's policies regarding the protection of personal information.

Currently SaskPower does not disclose to the public the name of the individual(s) responsible for privacy and the management of personal information.

SaskPower outsources the processing of all customer service information with Information Systems Management ("ISM"), which includes the printing and mailing of customer statements along with SaskEnergy's as ISM also processes SaskEnergy's customer information. SaskPower's contract with ISM addresses the issue of protecting the personal information housed and processed by ISM.

SaskPower's Customer Services Directive and Release of Information Policies establish procedures for responding to complaints and inquiries regarding personal information.

11. SaskPower (continued)

IDENTIFYING PURPOSES

SaskPower has identified the types of personal information it collects and has classified the personal information it collects according to its sensitivity.

The most sensitive personal information housed by SaskPower is stored on the Customer Services Information System (“CSIS”). Electronic information is protected by restricted security access as authorized by data owners.

Access to information is determined by the business unit data owners. The Corporate Information & Technology (“CI&T”) Security department administers the access based on the approval of the data owners. The Vice President of Customer Services is responsible for all Customer Services personnel who access customer data. The Manager of Call Centres and Collections is responsible for the approximately 200 people who have access to CSIS in order to perform the functions of processing applications for service, answering billing inquiries, processing payments, etc.

The Supervisor, Business and Applications Support, Customer Services is responsible for overseeing the functioning of CSIS in conjunction with support personnel assigned by the CI&T department.

SaskPower does not create personal profiles by combining personal information from various sources.

The majority of residential, farm and commercial customers are advised verbally at the time of a new service application or a tenancy change application that SaskPower requires certain personal information in the event that they need to contact the customer for important or urgent issues. It is also implied that personal information will be used to provide services to customers and for billing purposes.

When a new technology or system is implemented SaskPower allocates resources to perform a risk analysis and requires the sign off of business requirements by Management/Supervisors before an application is in production and ultimately is implemented.

New employees are given training and all employees receive verbal one-on-one coaching regarding how to describe to customers what the personal information being collected is going to be used for. In addition, SaskPower will periodically issue emails to staff from supervisors to clarify how to approach particular situations.

11. SaskPower (continued)

CONSENT

Consent to collecting personal information is generally implied consent when customers apply for services or make changes. Customers can refuse to give SaskPower information. In exceptional circumstances SaskPower may refuse to process a service application request until they obtain some minimal information such as a phone number and contact name for reaching the customer. If a customer asks why personal information is being gathered, SaskPower will explain the reason for the gathering of the information.

By process SaskPower only uses the personal information for purposes of providing services to its customers, billing customers and collecting payment from customers.

SaskPower will gain written consent from individuals prior to disclosing personal information to any third party unless the third party is a government department, a fellow Crown Corporation, the Sheriff's Office or a police force.

LIMITING COLLECTION

SaskPower only gathers the information dictated by the data fields of CSIS to ensure that only the personal information needed by SaskPower is collected.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

SaskPower staff is required to follow the Corporation's Code of Conduct policy, which stipulates that personal information is only to be used for the purpose it was originally collected.

SaskPower has formal procedures in place with respect to the retention of personal information. CSIS automatically deletes accounts finalized and paid in full after 3 months. Accounts finalized but not paid are kept electronically for 7 years. Microfiche records are kept, which go back farther than 7 years, but generally not beyond 10 years.

MAINTAINING ACCURACY

Front-line staff is instructed that when they deal with a customer on any matter, they are to reconfirm with the customer that SaskPower's personal information is still correct.

11. SaskPower (continued)

SAFEGUARDS

In order to safeguard and protect personal information from unauthorized access, disclosure, copying, use or modification SaskPower controls access to CSIS. Access to CSIS is only obtained through the System Administrator, currently the Supervisor, Business and Applications Support, Customer Services. Access is assigned in consultation with the hiring supervisor or manager based on job function.

When a staff member is terminated the department manager and/or human resources will notify the system administrator to remove the individual's access to the system. When staff changes roles in the Corporation, the hiring or leaving manager will notify the system administrator of any required changes. External and internal auditor's will periodically review employee's access rights to ensure that they are consistent with the employee's role.

Front-line staff is required to sign-off the system at the end of the business day. At Head Office, staff has access badges, which only allow them into authorized areas. PIN numbers are required for access to the computer room after hours. Areas where sensitive information is housed are in locked areas. Security cameras with commissionaires monitor SaskPower's head office 24/7/365. There is a restricted list of who can recall offsite tapes.

Passwords, firewalls and strong authentication for remote Internet access processes are used to protect personal information.

Third parties, including contractors, suppliers, partners, etc. with whom personal information is shared are required to sign confidentiality agreements.

Employees currently do not sign confidentiality agreements; however, SaskPower plans to implement a new policy in the fall of 2002, which would require all new employees to sign a confidentiality agreement. On an annual basis, SaskPower circulates the Code of Conduct to all employees and it is available electronically on the corporate Intranet.

In order to improve privacy and security SaskPower participates in all Government of Saskatchewan Security Charter group meetings.

OPENNESS

SaskPower will communicate either verbally or in writing to the public, depending on the nature of the request and how it is submitted, what its policies and procedures are in regards to personal information.

11. SaskPower (continued)

PROVIDING ACCESS

SaskPower allows individuals to access their personal information. Information routinely released to customers includes billing and consumption information. Requests for such information is handled by regional front-line staff or out-of-scope Supervisors.

SaskPower undertakes to confirm that the person they are releasing the information to is the customer. SaskPower requires written permission from the customer to release information to a third party (example, a real estate agent wanting consumption information for a residence). An exception where written consent is not obtained includes releasing personal information to authorized agencies previously noted. Since 1999 any requests for personal information are dealt with by senior staff members.

If the authority to release the personal information is unclear SaskPower's Legal Department will provide advice.

Supervisors have recently verbally instructed staff to record the name of the recipient and the date information is released on CSIS when information is released.

When personal information is shown to be inaccurate, typically by information provided by the customer either verbally or in writing, the information is amended based on the information supplied. Consent to making any amendments is implied in the customer providing the information.

CHALLENGING COMPLIANCE

SaskPower has a formal process in place for those circumstances where an individual or entity feels that they should have access to information, which SaskPower has refused to give.

Complaints that an employee has inappropriately released information are dealt with in the same fashion as any complaint about an employee's conduct. The out-of-scope supervisor or manager investigates the matter and confers with the Vice-President as to appropriate actions.

SaskPower reports it has not received any complaints regarding its personal information management practices in the past 12 months. With the exception of the recently reported issue of an employee(s) allegedly releasing information to third parties who may not have held appropriate authorization, Sask Power reports no further evidence of policies pertaining to the handling of personal information being breached in the past 24 months.

11. SaskPower (continued)

RECOMMENDATIONS

1. SaskPower should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. SaskPower should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. SaskPower should disclose to the public who is responsible for privacy and who is responsible for the management of personal information.
4. In the development of contracts with outside parties, SaskPower should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the corporation provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the corporation's personal information (privacy) requirements.
5. SaskPower should evaluate the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. SaskPower should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed.
7. SaskPower should implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
8. SaskPower should implement regular reviews to ensure compliance with *FOI* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
9. SaskPower should review current information collection, retention, handling and destruction procedures to determine if any changes are needed based upon privacy best practices.
10. SaskPower should consider having employees review the privacy policy annually and obtaining an annual signoff from employees identifying that they understand the principles of privacy.

12. Saskatchewan Liquor and Gaming Authority

INTRODUCTION

As a regulator and a retailer, Saskatchewan Liquor and Gaming Authority (SLGA) collects and uses a variety of personal information. Listed below are the five main areas in which SLGA collects and uses personal information:

Licensing and Regulation of Gaming

In order to license and regulate gaming under *The Alcohol and Gaming Regulation Act*, SLGA collects and uses personal information to assess the good character and suitability of gaming employees and suppliers of gaming and non-gaming goods/services. Information collected can include an individual's criminal history, civil proceedings history, marital information, residential history, education and training, employment history, finances and financial history, and any other information deemed necessary to determine whether the applicant is of good character and suitability.

Licensing and Regulation of Alcohol

In its alcohol regulatory role, SLGA also collects personal information. In addition to obtaining name and address information for liquor permit outlets and licensees, SLGA collects information on the owner's (or in case of corporations, major shareholders) criminal history.

Licensing and Regulation of Horse Racing

Individuals seeking licenses in horse racing are required to submit personal information as part of the application process in order for SLGA to assess whether a license should be issued. Information collected includes an individual's financial affairs, criminal history and employment history.

Video Lottery Terminal (VLT) Program

In operating the VLT program, SLGA allows VLTs only in age-restricted, liquor-permitted establishments. In order to qualify for VLTs, the owners of these establishments (or in the case of corporations, major shareholders) must provide SLGA information on their criminal history. In addition to the owners, any staff of the establishment that have been assigned responsibility to interact with the VLTs (e.g., staff with keys to open machines to change tape and collect cash) must provide SLGA information on their criminal history.

12. Saskatchewan Liquor and Gaming Authority (continued)

Retail Liquor Operations

As part of its liquor store operations, as with any retailer, SLGA collects credit card and debit card information from its customers who choose to use this form of payment. The use of this information is limited to completing the financial transaction and obtaining the necessary funds from the customer's creditor or bank.

As well as part of its liquor operations SLGAs contracts with individuals or entities to sell liquor. These individuals/entities are called liquor vendors or SLGA franchisees. In applying for a franchise, individuals are required to complete a "Liquor Franchisee Application and Personal History Report". The application requests information including the individual's criminal history and previous employment. In addition, SLGA requires individuals to provide information relating to their credit worthiness prior to entering into a franchisee contract.

In its normal course of business, SLGA receives and stores names, addresses and phone numbers. These can be collected as part of the activities listed above or through other activities such as registering organizations for charitable gaming activities, and receiving and responding to correspondence from a variety of individuals whether they be members of the public or stakeholders.

SLGA does not collect information on behalf of another department, agency or level of government. Within SLGA, personal information is shared between SLGA branches involved in the regulation and licensing of gaming and liquor activities. For example, the results of a Canadian Police Information Centre (CPIC) inquiry and investigation work by the Compliance Branch may be shared with the Charitable Gaming or Liquor Licensing Branch for the purposes of licensing while financial information may be shared with the Audit Services Branch for the purposes of assessing a gaming supplier's financial viability.

SLGA does share personal information with other government departments or agencies. For example, on rare occasions, in order to assess the good character and suitability of a gaming employee or supplier, or to assist another gaming jurisdiction make an assessment of an applicant in their jurisdiction, personal information is disclosed to another jurisdiction (i.e., gaming regulators). Disclosure of such information is covered by a consent to release form. Information is also shared if a Memorandum of Agreement to share information is in place with another jurisdiction.

12. Saskatchewan Liquor and Gaming Authority (continued)

As well, under an agreement to share information, SLGA agrees to provide Social Services, in an electronic format, the names, addresses, position occupied, place of employment and social insurance number of gaming employees registered pursuant to section 98.8 of *The Alcohol and Gaming Regulation Act*. This agreement has been inactive, as no information has been exchanged under it in the last couple of years. Also, on rare occasions, personal financial information (e.g., raffle winnings) is released to Social Services when Social Services provides SLGA a copy of a signed release from the individual in question supporting Social Services request for such information.

On rare occasions, personal information has been released under section 29(2)(f)(i) and (h)(i) of *The FOI Act* which allows for the release of personal information for the purpose of complying with *The Canada-Saskatchewan Tax Collection Agreement*.

SLGA receives personal information from other departments/agencies/levels of government. For the purposes of assessing the good character and suitability of gaming employees and suppliers, information is obtained from the Canadian Police Information Centre (CPIC). As well, information may be received from other gaming jurisdictions (as described above). SLGA obtains a release from individuals to obtain this information.

SLGA uses *The FOI Act* as its guide and reference in determining what is personal information. This act also governs SLGA with respect to personal information. SLGA has also been prescribed by section 14 of *The Freedom of Information and Protection of Privacy Regulations* as an investigative body to which personal information may be disclosed with respect to investigations pursuant to acts and regulations it administers and any laws of Canada that it enforces.

The Alcohol and Gaming Regulation Act provides direction and authority for SLGA to license and undertake investigations, and obtains information with respect to its investigation and licensing activities.

The management of personal information at SLGA is also affected by policy and procedures that are in place to ensure compliance with the terms and conditions of *The Memorandum of Understanding between the Saskatchewan Liquor and Gaming Authority Licensing Division, Compliance Branch, and the Canadian Police Information Center (CPIC)*.

12. Saskatchewan Liquor and Gaming Authority (continued)

ACCOUNTABILITY

There has not been an individual charged with formal responsibility for privacy at the department. The Executive Director, Policy and Planning Division, is responsible for managing SLGAs responsibilities and enquiries made under *The FOI Act*. The division provides guidance and direction to SLGA staff when issues arise with respect to the protection and release of personal information.

In addition, branch managers are responsible for the policies their branch uses to protect personal information collected and maintained by their branch. The branches who primarily collect and use the personal information include Compliance, Charitable Gaming, Liquor Licensing, Horse Racing, Casino and Electronic Gaming, and Audit Services.

Upon request from the public, the identity of the Executive Director, Policy and Planning Division, is made known to the public.

SLGA does not outsource any processing of its personal information.

Written policy and procedures exist at SLGA with respect to personal information gained through SLGAs access to CPIC and investigations undertaken by SLGAs investigators.

These policies are available to the public and SLGA does tell individuals of these policies when appropriate. If a member of the public asks if such policies existed or could be released, SLGA would provide the policies upon request.

The written policies mentioned above are used primarily by SLGAs inspectors and investigators. The policies and procedures are used by these employees in the normal course of their work with each individual having access to a copy of the branch's policy and procedures manual. As a result, communication of the above policies occurs as part of the individual's daily job.

On occasion e-mails are sent to these employees reminding them of the importance of protecting confidential information, personal or otherwise.

Formal training or awareness sessions have not been held to inform employees about the protection of personal information. However, protection of personal information can be raised and discussed at branch meetings. As an example, SLGAs Compliance Branch, which conducts investigations and CPIC enquiries, frequently discusses at its branch meetings the protection of personal information.

12. Saskatchewan Liquor and Gaming Authority (continued)

SLGA has established procedures to receive and respond to complaints and inquiries. Freedom of information inquiries, which at times include requests for personal information, are routed to the Policy and Planning Branch which is responsible for responding to freedom of information inquiries. These inquiries are logged and assigned a file number. Formal complaints are generally received through the CEO's office. Freedom of information inquiries are logged and tracked.

General complaints and inquiries relating to liquor or gaming activities are tracked and logged by the Compliance Branch. All complaints are given a file number and recorded in a ledger for investigation. Diary dates are assigned to ensure timeliness of investigation and response.

Security card access is required to access SLGA work areas in order to protect personal information.

With respect to protecting gaming registration and CPIC enquiries/results which SLGA considers as some of the most sensitive personal information it maintains or has access to:

- Access to the registration area is restricted (locked room). The room is locked at all times when not occupied by authorized personnel.
- The CPIC terminal is located in the restricted area. The room has keypad access only. Access to the room is restricted to registration personnel and the Executive Director and Supervisor of Compliance Branch.
- The CPIC monitor and printer are positioned to prevent observation by unauthorized persons.
- The CPIC terminal is left on alternate route when not in use or when left unattended.
- "Confidential" is stamped on all reports as identification.
- All applications for gaming employees and suppliers pass directly to Compliance Branch for opening and are not opened in SLGAs common mailroom.

Audit Services Branch also receives confidential and personal information. Within Audit Services, laptop computers are locked in a cabinet or in an office at night. Paper files are locked in offices or cabinets at night.

Compliance with SLGAs written and unwritten policies and procedures are monitored by branch managers and supervisors in the normal course of daily operations.

12. Saskatchewan Liquor and Gaming Authority (continued)

IDENTIFYING PURPOSES

The process used to determine what personal information SLGA maintains is as follows: *The Alcohol and Gaming Regulation Act* requires SLGA to determine good character and suitability in a number of instances. The determination of the type of information that is necessary to assess good character and suitability for a particular type of permit, registration or license is a senior-level policy decision. *The Alcohol and Gaming Regulation Act* provides guidance in making these decisions (e.g., sections 28 and 44) and specifies some of the types of personal information to be collected (e.g., criminal record history).

As discussed previously, various levels and types of personal information are gathered to determine if an individual is of good character and suitable to undertake the activities in question. This information is maintained on file to support the registration or licensing of individuals (or denial of a registration or license as the case may be).

SLGA currently does not identify and classify personal information according to its sensitivity. All personal information is treated as confidential regardless of the type of personal information collected. To date, privacy protection has not been formally implemented.

Some of SLGAs most sensitive personal information is with respect to gaming registration and CPIC enquiries/results. This information is housed in a locked room that has keypad access only. Only restricted personnel (5 individuals) have access to this room. Furthermore, to access the room, one must enter SLGAs common work area, which is protected by security card access only.

Criminal history information associated with accessing an individual's suitability to hold a liquor license is maintained in filing cabinets in SLGAs work area, which is protected by security card access.

Horse racing file applications, which can include criminal history information, are maintained in the manager's office in locked filing cabinets.

Individuals have been assigned to be responsible for gaming registration and CPIC inquiries, Liquor licensee applications and horse racing applications.

SLGA does create personal profiles by combining personal information from various sources. In order to make an informed judgment on an applicant, they use the application, put it in a file, perform a CPIC check, etc.

12. Saskatchewan Liquor and Gaming Authority (continued)

SLGA does notify individuals in advance why their personal information is going to be collected and how it will be used. Personal information is collected when individuals apply for registration or a license. When applying, individuals fill out application forms, which contain a section that requests the applicant's consent to obtain personal information. These forms also explain what the information will be used for.

In addition, given the nature of what the individual is applying for, it is self-evident that the personal information is being collected to determine their suitability for the registration or license they are applying for.

When implementing new business processes SLGA usually undertakes a team approach to redesigning and building major new business process. This includes individuals from the business unit affected by the change and SLGAs Audit Services Branch. Individuals from the business unit are familiar with the personal information collected and used with respect to the business process under review and are aware of what type of safeguards must be built into any new process to ensure the protection of personal information.

The Audit Service Branch is also usually involved not only as an independent third party but as specialists. Their role is to ensure appropriate internal controls are built into new business process to ensure the integrity of the process and ensure appropriate controls are in place, not only over personnel information, but for all aspects of the new business process.

When implementing a new technology, SLGA uses a variety of security of features including security software, firewalls, hardware configurations, and passwords to protect personal information.

Individuals at SLGA are trained on the job on how to describe what the personal information collected is going to be used for. Generally, information is collected and used by the same individuals. As a result, the individuals are familiar with what type of information is required, why it is collected, and how the information will be used once collected.

CONSENT

Written, informed consent is received as part of the gaming/liquor application process.

12. Saskatchewan Liquor and Gaming Authority (continued)

In addition, individuals are required to sign the application forms on which they include their personal information. Providing personal information is part of the application process. The consent is recorded on various consent forms that individuals are required to sign. Users of the personal information are informed of the personal consent through the consent forms. The forms are part of the registration process and are included in the file that includes the individual's personal information.

Branch managers and supervisors are responsible for ensuring personal information is used for the purposes intended.

For CPIC inquiries and investigations undertaken by SLGA inspectors and investigators, the manager and supervisors of the branch monitor investigations and sign off on the investigation when it is completed. Furthermore, the use of CPIC by SLGA is audited by the RCMP.

SLGA does inform individuals and gain consent when disclosing their personal information to third parties. The consent forms used by SLGA state that personal information can be shared with a third party for the purposes for which the information was collected.

If a freedom of information inquiry is received requesting personal information, the information is not released unless the individual is contacted and their written consent is received to release the information.

Third party information is also released if required by law. An example of such is SLGAs sharing information with law enforcement agencies such as the RCMP pursuant to a memorandum of understanding prepared in accordance with *The FOI Act* to assist those enforcement agencies with lawful criminal investigations.

Normally, information is not used for any purpose other than that described on the consent forms. However, if an occasion arose that a different use of the information was required than originally intended, approval from the individual would be sought for the use not previously identified.

LIMITING COLLECTION

In order to ensure that the organization only asks for the personal information it requires, the standard application forms outline the information required to process a registration or license request. The consent forms also describe the information SLGA needs. The information requested has been determined to be the type of information necessary to make an assessment of the good character and suitability of an individual to hold a gaming or liquor registration/license.

12. Saskatchewan Liquor and Gaming Authority (continued)

This determination is made by reviewing what is required to ensure the provisions of *The Alcohol and Gaming Regulation Act* are being complied with. Information collected for this purpose is consistent with information collected in other jurisdictions with similar regulatory responsibilities.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

The organization ensures that the personal information is used for the purpose it was originally collected through the supervision of the branch manager and supervisor of the activities of their branch. They also do so through on-the-job training where staff are trained as to how to use the information received by SLGA. As well, access (i.e., physical) to the information is restricted. With respect to retaining and destruction of information, SLGA follows and uses the Saskatchewan Administration Records Systems (SARS) as its record retention policy.

The organization does collect information about individuals from third parties. In order to obtain information about the good character and suitability of an applicant, information can be collected from third parties such as character references, previous employers, and criminal history from the RCMP. Individuals consent to the collection of this information when they sign a consent form.

MAINTAINING ACCURACY

The organization does ensure the information it collects and uses is up to date and accurate. With respect to SLGAs gaming registration activities, applicants are required to provide updates to any changes in their personal history as part of their registration. Gaming registration information is also updated through the registration renewal process. This is verified as part of due diligence investigations conducted by SLGA and through annual CPIC reviews.

With respect to liquor licenses, SLGA requests updates on the status of individuals (shareholders) in companies on an annual basis. This is requested by sending out an annual renewal form.

All other personal information collected by SLGA is updated on an “as needed” basis.

12. Saskatchewan Liquor and Gaming Authority (continued)

SAFEGUARDS

The organization does have safeguards in place to protect personal information from unauthorized access, disclosure, copying, use or modification. With respect to physical security measures, overall, security card access is required to access SLGA work areas.

With respect to gaming registration and CPIC inquiries/results which SLGA considers some of the most sensitive personal information it collects and maintains:

- Access to the registration area is restricted (locked room). The room is locked at all times when not occupied by authorized personnel.
- The CPIC terminal is located in the restricted area. The room has keypad access only. Access to the room is restricted to registration personnel and the Executive Director and Supervisor of Compliance Branch.
- The CPIC monitor and printer are positioned to prevent observation by unauthorized persons.
- The CPIC terminal is left on alternate route when not in use or when left unattended.
- “Confidential” is stamped on all reports as identification.
- All applications for gaming employees and suppliers pass directly to Compliance Branch for opening and are not opened in SLGAs common mailroom.

Audit Services Branch also receives confidential and personal information. Within Audit Services, laptop computers are locked in a cabinet or in an office at night. When on the road laptops are secured to a desk with a key lock mechanism. Paper files are locked in offices or cabinets at night.

Sensitive information relating to horse racing applications are kept in a locked filing cabinet or desk in the horse racing manager’s office.

Technologically, electronic information is protected by security software, passwords and firewall.

Employees are not required to sign confidentiality agreements with respect to protecting personal information but are required to sign the government’s standard “Oath of Allegiance” upon entering employment with SLGA. Third parties with whom personal information is shared are required to sign confidentiality agreements.

12. Saskatchewan Liquor and Gaming Authority (continued)

OPENNESS

Communicating the organization's policies and procedures regarding personal information is done so verbally. If the request is made in writing, it will be responded to in writing.

PROVIDING ACCESS

Generally, if a request by individuals for the release of their personal information is made, the information would be released. If the information relates to an SLGA investigation the information may not be released in accordance with *The FOI Act*.

SLGA does not release investigative files of any type, unless they are being used for a legal proceeding, which includes a Saskatchewan Liquor and Gaming Commission hearing. A ruling by Saskatchewan's Freedom of Information Commissioner has supported this practice.

One individual does not handle all the releases of information. If the request is made under *The FOI Act*, one of three individuals in SLGAs Policy and Planning Branch who have been assigned responsibility for handling such will respond.

If an inquiry is made directly to a program area and is not made under *The FOI Act*, an individual in the program area would handle this inquiry. Generally, the program staff would contact one of the three individuals above to seek direction and advice.

The organization is confident it can identify all personal information. As all information related to a particular application is kept in one file, SLGA is relatively confident that all personal information can be identified. In situations where an individual may be involved in more than one application and the individual does not identify this fact, there is a possibility that all personal information held by SLGA may not be identified. However, as such files are cross-referenced, the likelihood of this occurring is low.

In order to release personal information, a written request is required. If it is determined appropriate to release the information requested, it is released.

If the authority to release the information is unclear, individuals within SLGAs Policy and Planning Division who have been assigned responsibility for processing requests under *The FOI Act* provide advice to SLGA staff with

12. Saskatchewan Liquor and Gaming Authority (continued)

respect to the release of the information. If further expertise is required, SLGAs solicitor, or a Saskatchewan Justice solicitor's advice is sought with respect to the release of the information.

When the information is released, the information released, name of recipient and date of release are all recorded. Inquiries under *The FOI Act* are assigned a file number and all information and responses pertaining to the enquiry including the information released are filed under the assigned number.

Information released as a result of inquiries not made under the above act, are generally placed on the individual's (permittee/licensee) file.

SLGAs Policy and Planning Division is responsible for responding to freedom of information inquiries. When responding to inquiries, the "consent" and "identifying purpose" sections under *The FOI Act* are considered by SLGA when responding to enquiries.

When releasing information to an individual other than the individual the personal information relates to (belongs to), SLGA enters into an agreement with the third party or ensures the individual whom the information belongs to has consented to its release.

SLGA does update or add to an individual's information if it is shown to be inaccurate, incomplete or out-of-date. An individual's criminal history and other factors relevant to their license or registration are updated periodically. The updated information is gathered in similar fashion as to how the original information was gathered. Information received from CPIC is considered accurate. SLGA does gain consent from the individual when making amendments. As a condition to holding a liquor or gaming registration or license (part of the registration's/license's conditions), an individual is required to consent to SLGA monitoring their continuing suitability to hold a liquor/gaming license/registration.

CHALLENGING COMPLIANCE

SLGA does not have a formal process in place to deal with complaints about its personal information management practices or policies. Complaints of this nature would be documented on receipt and depending on the nature of the complaints would be assessed by the manager for a response at the branch level, or corporate level. Corporate level complaints would be handled by the Policy and Planning Division who have been assigned responsibility for *The Freedom of Information and Protection of Privacy Act*.

12. Saskatchewan Liquor and Gaming Authority (continued)

SLGA has not received any complaints regarding its management of personal information practices and policies in the past twelve months and is not aware of any breaches in policy or procedure pertaining to the handling of personal information.

RECOMMENDATIONS

1. SLGA should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. Once the overall government privacy framework is developed, SLGA should develop policies and procedures that support the overall privacy framework.
3. SLGA should establish overall accountability for privacy (as they have done with *The FOI Act*).
4. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.
5. SLGA should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.
6. SLGA should implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
7. SLGA should continue to conduct regular reviews now including compliance with *FOI* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
8. SLGA should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations. Following on this overarching policy, each Branch should review its current policy to ensure alignment with departmental policy.
9. SLGA should formalize the process they currently have to record what information was disclosed, shared, etc, in order to inform an individual of the specific information about them that has been disclosed.
10. SLGA should develop a formal process to deal with complaints.
11. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

13. Saskatchewan Property Management Corporation

INTRODUCTION

Saskatchewan Property Management Corporation (SPMC) is a Treasury Board Crown Corporation that provides accommodations and other central support services to government and other public agencies.

SPMC is responsible for the maintenance of over 1,300 provincially owned or leased facilities in the province of Saskatchewan and provides support services to other government agencies such as a central vehicle agency, telecommunications support services, mail services, conference facilities, purchasing and a distribution centre for office, janitorial and health supplies.

SPMC collects and retains personal information in the course of its business activities. For example, SPMC may conduct inquiries into the financial background of individuals (it also does so with respect to various corporations) with whom the Government of Saskatchewan is considering doing business in order to ensure that these persons are able to meet contractual obligations without placing public funds at risk. Such reviews are conducted pursuant to SPMCs *Investigative Services Policies and Procedures Manual*. SPMC also collects personal information in that it requires security screening for its employees and for any contractors working within the ambit of property management in federal government buildings managed by SPMC and at the Echo Valley Conference Centre when the DND Sea Cadet Program is in progress.

SPMC Records Management is the central storage area for the Government of Saskatchewan. Records Management operates in a secure building separated from other government departments and agencies.

Two senior employees have been designated as Special Constables pursuant to the *Saskatchewan Police Act*, which allows them access to personal information usually reserved for police officers. This is required in order for the designated SPMC officials to provide investigative services to various government departments and agencies. Prior to obtaining police criminal record information, consent is often sought from the individual involved, although it is recognized that such a protocol is not always practical or appropriate, depending on the nature of the investigation being undertaken. A limited number of SPMC employees are also authorized to receive Registered Vehicle Owner's information from Saskatchewan Government Insurance (SGI), to assist in responding to parking violations at lots owned by SPMC in Regina.

13. Saskatchewan Property Management Corporation (continued)

ACCOUNTABILITY

Responsibility for managing departmental policies pertaining to personal information is shared as follows:

Investigative Services Policies and Procedures Manual

The Director of Legal and Risk Management Services (LRMS) is accountable for managing the policies and procedures contained within this manual. The Director of LRMS is responsible for directing the legal, investigative and risk management services to the Corporation on its business activities.

Code of Conduct

Director of Human Resource Services (HRS) takes the lead role in either the facilitation of development, or actual development, of policy applying to employees of the Corporation. HRS is responsible for ensuring policies are within the framework of the applicable legislation and collective agreements.

Human Resource Policy Manual

Director of Human Resource Services – see comments above

Security Policy and Procedures Manual

The Chief Information Officer and Vice President of Information Technology Division are responsible for setting standards for the protection of SPMCs Information Technology Systems, including the Government e-mail system. A Security Committee, comprised of the Information Technology Security Administrator, the Director of Legal and Risk Management Services, the Director of Protective Services and the Director of Telecommunications, assesses risks to SPMCs systems and maintains the Security Policy and Procedures Manual.

SPMCs corporate Internet website contains information related to all of the corporation's services as well as contact names and telephone numbers. No outsourcing of IT or other processing takes place.

In those instances where third parties are contracted to provide services to SPMC and where that third party has access to personal information in the course of the engagement, SPMC policy is such that the third party must agree not to disclose such information without the consent of SPMC, except as required in the course of carrying out the engagement. Policy is set out in the SPMC Security Policy and Procedures Manual – "Security Obligations of Consultants and Other

13. Saskatchewan Property Management Corporation (continued)

Parties” (Page 10) and “Contracting with Consultants and other Service Providers” (Page 22). A “Confidentiality Agreement for Contractors” was developed and is used by the Telecommunications Branch.

Discreet policies respecting personal information are also available in the SPMC Security Policy and Procedures Manual, the SPMC Code of Conduct, the SPMC Investigative Services Policies and Procedures Manual and the SPMC Human Resource Policy Manual.

Contents of applicable manuals are communicated to staff by several means. Copies have been distributed to managers and directors for staff discussion. They have not been placed on the Internet for access by the general public. Employees having access to the SPMC computer system were required to sign and submit the Information Security User Agreement. A brochure and video were also produced and made available to staff.

The SPMC Code of Conduct was introduced in April 2000. The Human Resource Policy Manual is regularly updated. Managers are asked to ensure that staff is aware of amendments.

Although no formal training sessions have been delivered, Legal and Risk Management staff responsible to receive, handle and store personal information signed the acknowledgement of responsibilities form on June 6, 2000 (included in the Investigative Services Policies and Procedures Manual). The results of investigations are not disclosed or discussed with anyone other than those persons associated with SPMC and other public agencies and government funded organizations who have a legitimate need to know in order to perform their duties.

The SPMC Security Policy and Procedures Manual sets out a process for staff to follow in the event of an incident occurring that threatens the security of information (including personal information), assets or personnel (See Security Policy and Procedures Manual – Incident Reporting, page 8).

The SPMC Internal Auditor audits compliance with policies and procedures yearly.

13. Saskatchewan Property Management Corporation (continued)

IDENTIFYING PURPOSES

No formal process is in place within SPMC to determine the amount and nature of personal information maintained by SPMC, nor is there a classification system to determine the relative level of threat/risk to which a given document is exposed. SPMC is awaiting the introduction of an overarching pan-governmental document classification system.

Some guidance is in place, however, with respect to defining the level of sensitivity of personal information and other documents. The Saskatchewan Administrative Records System (SARS) defines a “confidential record”. SPMC has in place a “need-to-know” process on an *ad hoc* basis.

SPMC reports that it does not aggregate data from various sources to create personal profiles on its clients, however, it does hold personal information from various sources when conducting a security screening check on an individual (see also the section headed Maintaining Accuracy, *infra*). Consent is usually obtained prior to conducting a criminal records check, however, in some instances consent is not sought if it is deemed that to do so may jeopardize an investigation. SPMC collects only minimal personal information.

Policy dictates that SPMC users are only to be provided access to those e-systems required to carry out their required duties and functions.

CONSENT

Consent is obtained prior to conducting security screenings (which includes a criminal records check), but not necessarily prior to conducting a credit check. The nature of some investigations makes it impractical to obtain consent from an individual prior to obtaining information from police agencies, e.g. when an individual appears to represent a security risk.

Consent, when it is obtained, is obtained by having the subject read and sign a specific consent form which explains the purpose for which the information is to be obtained and the subsequent use to be made of the information. In the case of security screening, the applicant is made aware that his or her information will be provided to the federal Department of Public Works and Government Services Canada.

LIMITING COLLECTION

Policies and Procedures set out in the Investigative Policies and Procedures Manual govern the use made of personal information collected and require that the information be used for the purpose(s) for which it was collected.

13. Saskatchewan Property Management Corporation (continued)

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

Information is managed pursuant to the *Archives Act* (Saskatchewan) and the *Freedom of Information and Protection of Privacy Act* (Saskatchewan). The former act (in conjunction with the Saskatchewan Administrative Records Classification System (SARS)) governs the retention and destruction of records while the latter deals with access to information held by the government.

Various SPMC manuals also govern the retention and disposal of records. These include the Security Policy and Procedures Manual – “Disposal of Sensitive Documents”, “Disposal of Computer Parts”, “Electronic Mail Backup” and the SPMC Investigative Services Policy and Procedures Manual - “Handling of Information”.

MAINTAINING ACCURACY

Legal and Risk Management Services endeavours to ensure that the personal information being collected, used and disclosed is as accurate and complete as possible. SPMC uses only the most reliable information sources in gathering data and is confident that the information is as up-to-date, accurate and complete as possible. Often, more than one information source is utilized. Information is then compared for accuracy and completeness.

SAFEGUARDS

SPMC Protective Services has established building security guidelines and set standards for the Corporation. These guidelines, covering all aspects of perimeter security as well as information on locks, hardware and key control, are used by programs to address physical security requirements and provide staff with important information on asset protection measures.

Investigative files are stored in locked file cabinets (utilizing locking bars and combination locks) and housed in locked offices. Electronic information is stored on secured network drives accessible only by authorized LRMS staff and IT Network Administrators. Electronic records are firewall and password protected. Storage is governed by Investigative Services Policies and Procedures (“Collection, Use and Disclosure of Personal Information”).

Human Resource Services receives and stores personal resumes of individuals seeking to obtain employment at SPMC. The resumes are kept for three months and then shredded. The documents are stored in locked filing cabinets and access is restricted to the Director of Human Resources and the Human Resource Consultants.

13. Saskatchewan Property Management Corporation (continued)

Employees are required to sign an Oath of Office when hired. No annual sign off is required. Third parties/contractors must agree as a term of their contract that they will:

- Not disclose sensitive data that they may be given access to during their employment
- Protect confidential information that has been entrusted to them by SPMC as though it was their confidential information
- Not divulge any information to any third party without the verbal or written consent of SPMC except as required in the course of carrying out services under the contract

SPMC is a charter signatory to the Government of Saskatchewan's Security Charter in 1999. The ITO in cooperation with the Systems Management Council developed the Security Charter. In signing the Security Charter, SPMC committed to raising the awareness and importance of security in the Corporation and addressing ways to improve the security of government information and infrastructure at SPMC.

SPMC is currently taking action to implement the recommendations of the Provincial Auditor in his 1999 and 2002 reports on Information Security.

OPENNESS

Policies, procedures, and points of contact are communicated to the general public in writing as requested. Members of the general public may also be provided with a printed copy of the policy(s) in question.

PROVIDING ACCESS

SPMC follows the applicable procedures with respect to the collection and disclosure of personal information, as outlined in *The Freedom of Information and Protection of Privacy Act* ("the FOI Act"). SPMC is confident that it is able to identify all personal information in its holdings with respect to any given individual. No personal information is routinely released. Release is accomplished on a case-by-case basis.

Requests for access routinely are channeled through the FOI Access Officer, who co-ordinates the release or denial of information. In the event release issues are unclear, the involved SPMC unit liaises with the FOI Access Officer. Requests for release of information are tracked within SPMC as per the FOI Administrative Procedures Guidelines.

13. Saskatchewan Property Management Corporation (continued)

Once collected, SPMC finds it has no need to amend or change information in its possession.

CHALLENGING COMPLIANCE

SPMC has no formal procedures in place to deal with complaints pertaining to its personal information management practices.

If an individual is refused access to a record or part of a record, or an individual requests that a correction of personal information and the correction is not made, they may ask the Information and Privacy Commissioner to review the decision. If the Commissioner reviews the matter and the individual is still not satisfied, the decision can be appealed to the Court of Queens Bench.

Further, the Office of the Provincial Ombudsman investigates complaints respecting administrative actions and decisions of government and, where warranted, recommends corrective action to the Government and the Legislative Assembly.

SPMC reports that it has received no complaints with respect to its personal information management practices in the past 12 months, nor has it experienced any breaches of policy or procedure in the past 24 months.

RECOMMENDATIONS

1. SPMC should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. SPMC should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan.
3. SPMC should establish formal accountability for privacy within the agency.
4. In the development of contracts with outside parties, SPMC should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where SPMC provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by SPMC's personal information (privacy) requirements.
5. SPMC should use the government's data classification scheme (to be developed) to determine the sensitivity of the information under its care. Given that the nature of the information held by the Department is relatively defined and static, this may not be a time consuming exercise for the agency. Policies should be developed to assist staff in determining the appropriate levels of safeguard for the information held.

13. Saskatchewan Property Management Corporation (continued)

6. SPMC should, along with the Government as a whole, evaluate the effectiveness of using implied consent (e.g. in completing an application form, the public has provided implied consent to the use of their personal information) rather than informed consent. As identified by the CSA principles, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used retained or disclosed.
7. Routine gathering of personal information to create a “background” on potential business partners, purchasers, etc., should be reviewed in terms of privacy best practices.
8. SPMC should continue to implement the information security recommendations of the Provincial Auditor to provide enhanced safeguards to personal information.
9. SPMC should continue to conduct regular reviews, including compliance with *FOI* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
10. SPMC should develop an overarching departmental policy to provide guidance with respect to the information collected, retained, handled and destroyed by the Department. This policy needs to balance the requirements identified in SARS with privacy considerations.
11. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
12. Formal procedures for handling and escalating complaints should be developed and promulgated.

14. SaskTel

INTRODUCTION

SaskTel collects, distributes and retains personal information pursuant to its Terms of Service (TOS). The majority of personal information collected is used for internal SaskTel purposes and is used in a manner consistent with the requirements of the *Freedom of Information and Protection of Privacy Act (The FOI Act)*. SaskTel uses personal information to market SaskTel products and services to the individuals from whom it is collected.

SaskTel has put in place and communicated to employees, policies and procedures pertaining to the collection and use of personal information. It should be noted that SaskTel, although a provincial undertaking, is regulated by the federal Canadian Radio Television and Telecommunications Commission (CRTC).

SaskTel receives and holds third party data in their data center and has contractual commitments with these business customers governing the confidentiality and use of that information. As this is written into the contracts, SaskTel does not provide their business customers with a statement as to how SaskTel protects the personal information entrusted to it.

ACCOUNTABILITY

An Information Officer manages *FOI* within SaskTel. Information concerning access to personal information is readily available publicly. Assistance is provided to members of the public who wish to access personal information held by SaskTel.

In those instances in which SaskTel contracts with outside third parties who must take receipt of personal information, SaskTel requires that a confidentiality clause be included in such contracts to recognize and protect the confidentiality of the information.

All SaskTel employees are made aware of the corporate Code of Conduct and the standard of behavior expected of them as employees. These requirements are again reviewed with each employee during the annual appraisal process. No annual sign-off to confirm that the employee recognizes the importance of protecting personal information is in place.

SaskTel monitors compliance with its policies pertaining to personal information through day-to-day interactions, through regular compliance audits and as part of the complaint process. SaskTel also employs a corporate compliance program to track any non-compliant activities to ensure that senior management are aware of any non-compliant action and, where necessary, to implement corrective actions.

14. SaskTel (continued)

IDENTIFYING PURPOSES

SaskTel has enacted a number of internal policies pertaining to the collection, use, dissemination and destruction of personal information. These are SaskTel policies, not overarching Government of Saskatchewan policies, which have been adapted. Policies assist SaskTel employees in identifying types of personal information to collect and to define the appropriate level of sensitivity and storage. The Security Director – Systems administers the overall policy.

The SaskTel privacy policy is posted on its web site. Employees receive training on the collection of personal information as well as the uses to be made of the information by SaskTel.

SaskTel creates personal profiles of its customers by making use of information collected primarily from individuals when they apply for service. Applicants are told in advance why their personal information is being collected and how it will be used. Consideration of the need to protect personal information is taken into account when new technologies or business processes are being considered.

CONSENT

Consent is always obtained prior to the collection of personal information from an individual. Specific, signed consent documents are not used, however, a notation is made to the client's account file. Corporate policies pertaining to the use of personal information are in place. Disclosures are made pursuant to the TOS, which in most cases requires written consent prior to release of personal information.

Consent is normally not obtained when personal information is used within SaskTel for business purposes not previously identified (ss. 28, 29 FOIPOP).

LIMITING COLLECTION

Collection is limited to that information which is needed for the purpose for which it was collected through adherence to *FOI*, corporate policy, the Code of Conduct, TOS and through employee training.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

SaskTel has in place a series of in-depth corporate policies with respect to collection, use and retention of personal information. SaskTel advises that the *Archives Act* of Saskatchewan does not apply to it, but the terms of the Act are followed generally. SaskTel retains information for at least a 6-year period after a customer ceases to be a customer.

14. SaskTel (continued)

MAINTAINING ACCURACY

SaskTel updates its customer profile on each customer contact. The customer confirms information.

SAFEGUARDS

Information is accessed on a need-to-know basis only. New employees require a criminal records check. SaskTel has enacted extensive policies aimed at ensuring that personal information is protected. These include a corporate Code of Conduct, a policy pertaining to building security as well as system security. Physical protections include a variety of locks and other control devices such as finger print readers, card readers and intrusion detection. Processes including firewalls, encryption and vulnerability assessments protect electronic information.

Contractors and other third parties who are required as part of their duties to access confidential information (which includes personal information) are required to sign a confidentiality agreement prior to such access being granted.

SaskTel has addressed the recommendations of the Provincial Auditor General's Fall 1999 Report.

OPENNESS

Privacy policies are posted on the SaskTel web site and in Informational Pages in the telephone book as well as in the TOS document.

PROVIDING ACCESS

SaskTel's access process is de-centralized in that all requests for access to personal information are not automatically channeled to the Information/FOI Officer, but are dealt with and information is released as appropriate at the lowest point possible in the corporate hierarchy. SaskTel policy is that an individual may access his or her own personal information at any time. If such access is permitted under the TOS, it is released to the individual after the SaskTel Customer Service Representative (CSR) has satisfied him or herself that the individual is who he or she represents him or herself to be. In the event of a situation arising, which the CSR is unable to resolve, the issue may escalate up the chain of command, culminating with the FOI officer.

Release to third parties is also governed by the TOS document. The customer is not contacted or notified when personal information is released pursuant to para. 69.4 of the TOS, which sets out the conditions and circumstances under which personal information may be disclosed.

14. SaskTel (continued)

Requests are usually directed toward a SaskTel representative such as a service representative or to the Information Office as a request for access to information.

Most information in the hands of SaskTel is released with the knowledge and consent of the customer, e.g. directory assistance. Release pursuant to and within the terms of reference of the TOS and *FOI* do not trigger an attempt to contact the customer to obtain specific permission for release.

CHALLENGING COMPLIANCE

SaskTel has in place formal corporate policies and procedures with regard to complaints. Complaints with regard to personal information are dealt with at as low a level as is appropriate in the circumstances. As necessary, the complaint may be referred up the management chain to the corporate Information Officer responsible for compliance with *FOI* principles.

During the period 2001 – 2002, there have been four formal complaints lodged with SaskTel relating to personal information. Breaches of policy and procedure relating to the handling of personal information were reviewed. Since 1998, three incidents have resulted in dismissal of an employee, two others have been suspended for periods of time and a letter of warning was issued to one SaskTel employee.

Managers rely on the SaskTel Code of Conduct and instill SaskTel policies and procedures in employees with respect to the handling of personal information.

RECOMMENDATIONS

1. As SaskTel's competitors fall under the federal privacy legislation (*Personal Information Protection and Electronic Documents Act (PIPEDA)*), which is based upon the CSA model code, we would recommend that SaskTel also adopt this code.
2. Taking into account number 1 above, SaskTel should assess the impact of the privacy framework that will be established by the government as a whole on the Corporation and respond accordingly.
3. SaskTel should establish overall accountability for privacy within the Corporation.
4. In the development of contracts with outside parties, SaskTel should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the corporation provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the corporation's personal information (privacy) requirements.

14. SaskTel (continued)

5. SaskTel should record all releases of personal information for other than inclusion in directories and use in billing in order to be able to indicate to the data subject to whom their personal information has been released.
6. Informally, SaskTel identified that customers are informed as to why their personal information is being requested. We recommend that this be formalized with a script, provided to SaskTel employees, when obtaining verbal consent for the collection of personal information.
7. SaskTel should ensure that regular reviews are completed to ensure compliance with *The FOI Act* and privacy principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
8. Based upon the sensitivity of the information determined by the data classification scheme developed by the government, as a whole, additional safeguards should be placed on highly sensitive data. SaskTel should evaluate the data in its care based upon this scheme, categorize the data and modify safeguards if necessary.
9. SaskTel should review current data retention and destruction policies and procedures and assess privacy best practices with respect to these policies for both electronic and paper documents.
10. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

15. SGI

INTRODUCTION

Saskatchewan Government Insurance (“SGI”) collects personal information on individuals to fulfill its mandate as required by the legislation by which it is governed. As identified by SGI, the organization administers *The Automobile Accident Insurance Act*, *The Vehicle Administration Act*, *The Highway Traffic Act*, *The Snowmobile Act*, *The All-Terrain Vehicle Act* and *The Motor Carrier Act* (collectively the Legislation).

SGI has also taken steps to prepare for the implementation of the *Health Information Protection Act*. For example, vehicle registration information (name, address, etc. of an identifiable individual) is collected and used by SGI for purposes of administering the Legislation. As well, due to a court decision, SGI will disclose the name and address of an identifiable individual shown in its records as the registered owner of a vehicle to collection agencies acting on behalf of private parking operators to collect outstanding parking ticket fees.

SGI collects information on behalf of the Department of Highways (permits and vehicle registrations) and the Department of Finance (tax).

SGI shares personal information with many agencies) who have applied and received permission to this information under *The Freedom of Information and Protection of Privacy Act (The FOI Act)*. The Auto Fund provides inquiry access to:

- bailiff services
- collection agencies
- financial institutions
- government agencies – Finance, Highways, Justice, Health, PEBA, SERM, Social Services, SaskPower
- Registrars of Motor Vehicles
- Other companies who have applied and received approval to receive information (e.g. vehicle sales, service or rental agencies)
- Cities of Saskatoon and Prince Albert, University of Saskatchewan for parking enforcement
- CCRA

SGI has developed “A Guide to Release of Information” which provides detailed instructions as to what employees are allowed to release and to whom. No personal information is allowed to be released to the general public. The Auto Fund shares information with law enforcement agencies. Information is provided to law firms provided the law firm has the signed authorization of the

15. SGI (continued)

individual or has a contract with SGI. Driver and vehicle information is available to all provincial and federal government agencies through direct access or a signed contract with SGI. Information may be released to private investigation companies for the purposes of legal proceedings arising out of the ownership, operation or use of a vehicle. A valid Private Investigators license must be presented and a contract with SGI for the release of information.

It should be noted that medical information is not released without the written consent of the individual.

SGI receives information from the Department of Health (medical appointment histories) and Information Services Corporation (lien checks).

SGI also carries on business in Saskatchewan as a competitive insurer under the trade name SGI Canada. SGI Canada collects, uses and discloses personal and other information for underwriting and claims settlement purposes.

SGI defines personal information as any information on an identifiable individual other than name. SGI also looks to *The FOI Act* to define personal information.

ACCOUNTABILITY

SGI's Freedom of Information Access Officer was identified. The Access Officer has corporate responsibility for managing corporate policies regarding personal information and overseeing compliance with such policies. Informally, the Access Officer also oversees privacy compliance but this process has not been formalized. SGI does have policies and procedures that apply to personal information under the organization's control.

SGI's Code of Ethics, Information Technology Policy, written decisions of its access officer, recommendations of the Information and Privacy Commissioner and case law serve as SGI's written policies or procedures with respect to personal information in its possession.

The Code of Ethics and the Information Technology Policy are publicly available. SGI would tell individuals about them where appropriate. Both of these policies were updated in May of 2002. The Code of Ethics and the Information Technology Policy are both available on the SGI intranet. The Legal Department has also held meetings with corporate staff to explain the Code of Ethics and Information Technology Policy. The Code of Ethics, Information Technology Policy and *The FOI Act* are all part of the SGI orientation program for new employees. There is also reference to and a brief explanation of *The FOI Act* in the Adjuster's Handbook.

15. SGI (continued)

SGI does have Confidentiality and Non-Disclosure agreements in place with the majority of third parties that it deals with.

They do not have specific privacy policies but do have confidentiality and non-disclosure clauses and follow the Freedom of Information Act. SGI has also considered the future implications of *HIPA*.

IDENTIFYING PURPOSES

Although not explicit, SGI only collects personal information in support of its mandates, such as the needs of the AutoFund to issue products, needs of other agencies (court, law enforcement, etc.). For the AutoFund division personal information collected is as follows: payment of claims, safety monitoring, medical, driver history, photo, and signature.

The Claims division collects name and address information, which is required for claims payment processing. Injury information is collected to properly assess the extent of injuries for certain benefits paid under PIP. Education and occupation information is collected to adequately compensate claimants for their income loss.

Any information that is health related requires the highest level of security. Security is then by claim type for adjusters and then by job function outside of claims. Claims of a sensitive nature or staff claims are pulled from general inquiry and set up with restricted access.

Electronically, SGI has various security schemes within their applications to restrict access for update, inquiry, part of inquiry or no inquiry. The most sensitive information (Health related) is restricted to injury adjusters or general adjusters working on bodily injury liability claims.

SGI does not explicitly tell individuals in advance why their information is being collected and how it is going to be used unless it is detailed medical information, for which the purpose is specified.

With the exception of fraud investigations, information is collected through application forms or medical records (which the individual has provided consent to SGI to obtain).

SGI has not formally documented the purposes for which personal information is collected with the exception of requests for disability benefits.

15. SGI (continued)

CONSENT

To bring themselves within legislation administered by SGI, individuals are obligated to provide personal information. For example an individual insured with a vehicle damage claim under Part III of The Automobile Accident Insurance Act must provide his or her name, address, vehicle license plate number and other personal information in order to obtain payment for his or her vehicle damage. Similarly an applicant for a driver's license under The Vehicle Administration Act must also provide personal information (e.g. name, address, date of birth, etc.) as a condition to obtaining a driver's license. In both cases the information is provided without consent of the individual but in compliance with legislation.

SGI does obtain the written consent of individuals with respect to the collection of personal information from third party sources through consent provisions found in application forms for:

- a. the benefits provided under Part VIII of The Automobile Accident Insurance Act
- b. policies of insurance issued by SGI (SGI Canada)

Most consent is implied as individuals are requesting services and are being told what is being done. They are not told how their information will be used, who it will be shared with, how long it will be kept, etc. Consent is not obtained for fraud investigations, as this is a potential criminal matter. Express consent is obtained for Application for Injury Benefits.

Where written consent to the collection of personal information is obtained it will appear in the application (for benefits or policy coverage) signed by the applicant. SGI staff using personal information collected with written consent will have access to the signed application. Third parties, for example medical and rehabilitation personnel, given access to personal information collected by SGI with written consent may not always be aware that specific consent for the collection (use and disclosure) of the information has been obtained.

Divisional managers are responsible for ensuring that personal information is only used in accordance with the consent obtained. Monitoring will commonly take the form of file reviews.

SGI only discloses personal information without the knowledge and written consent of an identifiable individual for those purposes covered under Section 29(2) of *The FOI Act* and the Regulations under that Act.

15. SGI (continued)

The Access Officer will either write to the individual requesting consent to disclosure of his or her information to a third party or require the third party to obtain the written consent directly from the individual.

SGI does not, as a matter of practise, use personal information for a purpose not previously identified. In cases of one of its insured's applying for insurance with another insurer or making a claim with another insurer, SGI will provide that insurer with some personal information on an individual without regaining the consent of the individual.

LIMITING COLLECTION

SGI, to some extent, must rely upon staff training and experience to ensure that only personal information required for use is requested. The corporation does however, offer guidance to staff on its personal information needs through underwriting manuals, claims manuals and application forms, all of which identify the personal information the corporation requires. Many of the application forms SGI uses are designed to gather personal and other information required by the legislation SGI administers. SGI does not collect information indiscriminately. They use the information that they collect to fulfill their mandates.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

SGI relies upon its Code of Ethics and Information Technology Policy to ensure that personal information is (with the exceptions previously noted under the heading "Consent") is only used for the purposes for which it was originally collected. Divisional management also bears responsibility to ensure that the use of personal information is only for the purposes for which it was originally collected.

SGI has no formal policy in place with respect to the retention and destruction of personal information. It does, however, have retention policies in place with respect to all information in its possession and control, which would include personal information.

For Printed materials

A number of informal policies are in place for the destruction of information, including personal information. The disposal of all paper is the responsibility of Manager, Admin Services (mailroom and warehouse).

15. SGI (continued)

Each department may employ a shredder to dispose of individual papers with personal information (typically of an ad hoc nature). The shredded pieces are put into bags with the normal recycling which is kept in an unlocked room in the parkade.

Each department also sets policy on how long to keep personal information (both client information and non-client e.g. rejected applications) in their paper systems. Files (Claims and SIU) are kept in the client area or at the Warehouse until retention dates arrive. Files to be destroyed are listed and boxed for shipment to the Shred Room. Imaged documents (Underwriting and Auto Fund) are boxed as imaged and stored in secure locations (time period of retention varies by area) until they are sent to the Shred Room.

The Shred Room is locked at all times. Keys are held by Facilities staff (they transport the boxes from various locations) and Mailroom staff (they transport some from the mailroom). Crown Shred & Recycling Inc. disposes of all SGI sensitive papers. Once per month, they pick up all paper in the Shred Room and dispose of it per policies set out in their contract (attached).

For electronic information

When SGI disposes of desktop equipment, the PC's hard drives are formatted. When SGI has a defective drive for servers, they wipe it. Tapes are destroyed by shredding via contract with Crown Shred & Recycling Inc. When info is no longer needed to be accessed or retained per the Archives Act, documents are destroyed.

SGI (SGI Canada) subscribes to a Canadian program known as the Habitation Insurance Tracking System (HITS) which maintains a database of insurance and claims history. SGI relies upon the signed application of its prospective insured to access this database. SGI also may obtain personal information from prior insurers. SGI will only solicit personal information from a prior insurer in cases where it is investigating and/or litigating a suspicious claim made against it by an insured. Subscription to HITS requires SGI provide insurance and claim history of their policyholders. It is very important to note that before SGI releases personal information to another insurer, they require that the other insurer have the written consent of the insured to obtain the information.

15. SGI (continued)

MAINTAINING ACCURACY

The AutoFund uses verification of identity documents, edits in system, legislation, updates from other agencies, and customers or issuing offices informing them of changes to information as the means to maintain accuracy. The Claims division maintains accuracy through the customers themselves and the credibility of medical information based on the reliability of the source. In the Underwriting division, the onus is on the insured to keep the division informed of the necessary personal information. Credit reports are requested annually on bond applicants in accordance with general industry practice.

SAFEGUARDS

SGI protects personal information through confidentiality and non-disclosure agreements that all staff, DWI contractors, issuers, external agencies and other MVD agencies are to sign. Non-disclosure wording is included in the standard Information Technology Professional Services Agreement and all other contracts are required to include non-disclosure wording acceptable to SGI.

Policies and procedures and a Code of Ethics identify an employee's responsibilities with respect to the confidentiality of personal information but not with respect to privacy practices. SGI considers all information that it holds to be confidential.

Physical claim files are stored at the adjuster's desk in file cabinets (no clean desk policy). The claims offices are locked in the evening. Each claims branch has a reception counter and the public does not have access unless they are ushered to an adjuster's desks.

Special Investigation Unit (SIU) have the following safeguards in place:

- SIU database (GIS): Locked file storage room, electronic access only, weekly access reports
- CPIC: Locked room, electronic access, security clearance by RCMP, data access by two staff only. Controlled and audited by RCMP – User Id & password protected
- IRIS (Regina Police Service information system): Locked room, electronic access, security clearance by RPS, User Id and password protected
- SIMS (Saskatoon Police Service information system): Locked room, key control and visitor log, security clearance by SPS, User Id and password protected

From a physical security standpoint, there is a corporate security committee that reviews and defines physical security. There are security guards and access controls in place.

15. SGI (continued)

All locations where files may be located are under lock and key outside of normal working hours. During working hours, staff are normally near the files. Master keys are carefully guarded. Locking filing cabinets are provided where departments determine information is confidential or sensitive.

At head office, card access controls are in place over the parkade and building after hours. The 9th floor computer operations center is under card access control 24/7.

Photo Id has been issued to all head office staff. Security guards are employed at head office to register every visitor and informal policies have been provided to the guards. IT Contractors are required to sign an Information Technology Professional Services Agreement, which includes a confidentiality clause.

On the technical side, user id/passwords, firewalls, encryption, secure socket layer, and a dial-back private network are used to protect electronic information. SGI has reduced system access to a need to know basis in preparation for *HIPA* legislation. SGI is also participating with the ITO on the Security Charter group in defining security policies and procedures

If an employee quits or is terminated from SGI authorities are revoked as part of the corporation's Human Resources exit process. A checklist regarding physical and data processing accesses is attached to the Termination Letter sent to the employee's Manager. If the employee is transferred or reassigned, changes are handled via established Corporate LAN Administrator procedures

OPENNESS

SGI has no process in place for communicating written or unwritten policies, procedures, contacts, etc. regarding information to those who request it or to the general public. Inquiries from the general public concerning the disclosure of personal information are dealt with at the departmental level or by the Access Officer.

PROVIDING ACCESS

Information about an identifiable individual is not routinely released. With respect to the AutoFund, on request from the customer, SGI may provide access to their personal information without going through the *FOI* process. Other departments frequently insist upon a completed *FOI* application before releasing file information to those individuals to whom the information relates.

15. SGI (continued)

Divisions are expected to handle all inquiries regarding the release of personal information. For example requests for vehicle registration and driver information are handled by the Information Services Department of the Auto Fund. Claims branch managers are expected to deal with requests for personal information received at the branch. Where an application as provided for in *The FOI Act* is received by the Access Officer, the Access Officer will request the information sought by the applicant from the division having possession or control of the information and conduct a review of the information. Copies of the discloseable information will be mailed out by the Access Officer under covering letter.

The Information Services Department of the AutoFund releases personal information (vehicle registration and driver information) both in writing and orally.

SGI Bodily Injury Units release personal information (medical and rehabilitation) by providing copies of the information to the individual to whom the information relates.

SGI does not record information released when released orally. In all other cases a record is maintained of the information released, the name of the recipient and the date released.

Where personal information is disclosed pursuant to an agreement between SGI and the recipient, the recipient is contractually bound to use the information for the purpose set out in the contract and to treat the information as confidential.

CHALLENGING COMPLIANCE

SGI has no formal process in place to deal with complaints about its personal information management practices or policies. Complaints concerning personal information management practices or policies are referred to the Access Officer for response.

The Access Officer has received two telephone calls over the last 12 months both related to disclosure of vehicle registration information (name and address) to collection companies for the purpose of collecting on parking tickets issued by private parking lot operators. In both cases, the Access Officer explained that SGI was legally obligated to release this information because of the decision rendered by the Court in GMAC v. SGI and the companion case City Collection v. SGI.

15. SGI (continued)

RECOMMENDATIONS

1. SGI should provide ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. SGI should assess the impact of the privacy framework that will be established by the government as a whole and respond accordingly.
3. SGI should consider adopting the fair information practices in the Federal Personal Information Protection and Electronic Documents Act (“PIPEDA”) legislation and to which all private sector insurance companies must comply by January 1, 2004.
4. In the development of contracts with outside parties, SGI should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the corporation provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the corporation’s personal information (privacy) requirements.
5. SGI should establish overall accountability for privacy within the organization.
6. SGI should incorporate processes, which explicitly tell individuals in advance why their information is being collected and how it is going to be used. They should formally document the purposes for which all personal information is collected. We recommend that SGI work with the HITS program to ensure that the privacy needs of individuals are balanced against the purposes of the program itself.
7. SGI should consider placing privacy statements on all forms. It may be done in the form of a brief “stub” statement and directions as to where the entire policy may be obtained.
8. When information is released to third parties (for example medical and rehabilitation personnel given access to personal information collected by SGI with written consent), the third party may not always be aware that specific consent for the collection (use and disclosure) of the information has been obtained. SGI should put processes in place to direct the third party to only use the information for the purpose in which it was intended under consent.
9. SGI should develop a formal policy in place with respect to the retention and destruction of personal information or include the specific types of personal information in the retention policies currently in place.
10. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.

15. SGI (continued)

11. SGI should develop processes for communicating written or unwritten policies, procedures, contracts, etc. regarding information to those who request it or to the general public. Develop privacy documents (such as pamphlets and brochures), clearly explaining the policies and procedures, which govern the protection of personal information. These should describe what personal information is held, how it is used and when it is disclosed to affiliates and third parties.
12. SGI should implement regular reviews to ensure compliance with privacy and *FOI Act* principles. This should include regular reviews of the safeguards in place to protect personal information (such as technology reviews).
13. SGI should record when information is released orally. This record should include whom it was released to and what was released.

16. Saskatchewan Health Information Network (SHIN)

INTRODUCTION

The Saskatchewan Health Information Network (SHIN) is a government agency created to facilitate the development of a province-wide health information network. This focuses on enhancing health services and the protection of personal information through legislation, policy and technical safeguards. SHIN is involved in ensuring that health information is made available to health providers in a timely manner. Access to personal health records is only granted to those providers within the province who have a specific need for information within the record in order to provide health care. Currently, SHIN only houses information and does not actually manage the information itself.

SHIN does not actively collect or share personal information. SHIN acts as a repository for information collected by health regions and other agencies involved in the provisions of health services which house the information on its servers. SHIN's servers are housed within SaskTel and are under strict access controls and protection as per the Master Service Agreement with SaskTel and Science Applications International Corporation (SAIC).

With respect to personal information, SHIN is governed legislatively under the *Archives Act* (Saskatchewan) and the *Freedom of Information and Protection of Personal Information Act* (*The FOI Act*).

SHIN has implemented numerous detailed policies and procedures with respect to the handling of personal information.

ACCOUNTABILITY

SHIN has identified and tasked senior employees in the Security, Operations and Corporate responsibility centres of the Department with overseeing and taking responsibility for policies concerning personal information. The identities of these persons are not known to the public, but they could be identified as necessary to deal with requests.

SHIN out-sources data centre management to SaskTel (the servers are housed in the SaskTel data center but SHIN retains complete control over the servers including access to them), while application management is out-sourced to a private contractor, SAIC. Each Master Agreement contains a confidentiality clause to protect the integrity of personal information in the hands of third parties.

16. Saskatchewan Health Information Network (SHIN) (continued)

SHIN has implemented detailed written policies and procedures with respect to the handling of personal information in possession of the Department. These policies and procedures are updated annually. Lunch and learn sessions are held for employees with each updating of the policies. In addition, employees are presented with a computer screen each time they sign on to the SHIN network, which reinforces the need to maintain confidentiality of personal information. SHIN employees typically do not access personal information, however, because SHIN acts as a repository for Saskatchewan health information their employees are, for the most part, technical persons who have no need to access specific data. Access to specific data is tightly controlled within SHIN. Employees are security cleared and closely regulated. All access to “live” data is monitored and electronically logged. In addition, the SHIN culture is one of best practices and professional pride in maintaining security.

The SHIN Help Desk logs complaints and/or inquiries. Procedures are in place to deal with any threat made to the integrity of the SHIN computer system. It should be noted that SHIN does not maintain paper records – all data held are electronic.

IDENTIFYING PURPOSES

The primary focus of SHIN is to ensure that the data in its control are secure. Data is the property of contributing health regions and other agencies involved in the provision of health services, thus, it is those regions and agencies to which an overall privacy framework applies. As a result, SHIN has implemented a detailed Security Framework Document, which discusses the nature of the system and the protection controls in place to ensure that data are secure and available to approved users when needed.

SHIN does not create personal profiles of individuals, nor does it dialogue directly with citizens of Saskatchewan concerning their personal information. This is more properly the role of whichever health region or agency that has collected the specific information.

CONSENT

SHIN does not collect information; therefore, it does not seek the consent of the individual involved. This responsibility for consent is relegated to the health region or agency, which collected the information. It should be noted that no owner of data has ensured that SHIN has signed an agreement to abide by their privacy policies.

16. Saskatchewan Health Information Network (SHIN) (continued)

LIMITING COLLECTION

SHIN retains and maintains information on behalf of health regions and other agencies involved in the provision of health services. The responsibility to ensure that information collected is within the nature and scope of acceptable practices belongs to the health region or agency, which collected the information.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

SHIN advises that this category does not apply to it for the reasons set out above. Retention of information is guided by the *Archives Act* (Saskatchewan). SHIN also has in place a detailed Disaster Recovery Plan as well as Customer Policies. SHIN does not destroy, erase or anonymize information in its possession because the information is the property and responsibility of the contributing health regions and agencies.

MAINTAINING ACCURACY

SHIN does not collect, use or disclose information. Accuracy is the responsibility of the contributing health regions and agencies.

SAFEGUARDS

Personal information is protected from unauthorized access, disclosure, copying, use or modification through the use of firewall protection, passwords and antivirus security. SHIN also makes use of Public Key Infrastructure (PKI) and VPN technology to encrypt transmissions of data. In addition, SHIN has negotiated detailed service agreements with third parties used by SHIN to process data.

SHIN conducts security clearance screenings on employees and requires confidentiality clauses to be inserted in all contracts. As noted previously, security clauses are contained within the Master Service Agreements with SaskTel and SAIC.

SHIN has completed a considerable amount of work with respect to its policies vis-à-vis the Fall 1999 recommendations of the Provincial Auditor. A detailed security policy has been implemented and is updated annually. Security awareness training has been included as an Action Item in the 2002 - 2003 Action Plan for SHIN. A checklist system is in place to ensure that employees who leave the employ of SHIN are required to return any security or access passes when their employment ends.

16. Saskatchewan Health Information Network (SHIN) (continued)

Physical security issues have been taken into consideration and modifications have been made in developing strategies within SHIN and the SaskTel data centre to protect data. SHIN is cognizant of issues surrounding the security and integrity of information in its possession. It recognizes that such security is the responsibility of the client health regions and agencies, and engages in dialogue with them to stress the importance of maintaining security. SHIN has identified and specified its mission critical systems. Corporate business continuity planning is in progress and will be included in the 2002 - 2003 Action Plan.

OPENNESS

SHIN does not communicate its policies to the general public since the public has no access through SHIN to information it holds for contributing health regions and agencies.

PROVIDING ACCESS

Data in the possession of SHIN belongs to the contributing health regions and agencies; therefore, SHIN is unable to provide access.

CHALLENGING COMPLIANCE

Any complaints made with respect to access to personal information would be forwarded by SHIN to the contributing health regions and agencies.

RECOMMENDATIONS

1. As SHIN holds information for the Health Regions, no recommendations apply specifically to SHIN.
2. It should be noted that contributing health regions and agencies whose personal information is held by SHIN are responsible for the privacy and security of the information that SHIN houses.

17. Social Services

INTRODUCTION

Social Services has a number of different divisions or branches within the department. The divisions can be classified as either program and services providers or divisions providing support to the divisions delivering services. Divisions, which deliver programs and services, include the following:

- Community Living Division
- Career and Employment Services Division
- Housing Services Division
- Child and Family Services Division
- Income Security Division

Divisions or branches, which provide support services to the program delivery divisions, include the following:

- Property Management Branch
- Research and Evaluation Division
- Financial Management Division
- Technical Services Division
- Information and Technology Division

In respect of personal information Social Services is governed by the following legislation:

- *The Child Care Act*
- *The Department of Social Services Act*
- *HIPA (Health Information Protection Act) (pending)*
- *FOI (Freedom of Information and Protection of Privacy Act)*
- *Child and Family Services Act*
- *Adoption Act*
- *Young Offender Act*
- *Public Health Act*
- *Mental Health Services Act*
- *Workers Compensation Board*
- *Public Service Act*
- *The Emergency Protection for Victims of Child Sexual Abuse and Exploitation Act*
- *The Archives Act*
- *The Donation of Food Act*
- *The Intercountry Adoption (Hague Convention) Implementation Act*
- *The Social Workers Act*
- *The Rehabilitation Act*
- *The Residential Services Act*
- *The Saskatchewan Assistance Act*
- *The Saskatchewan Income Plan Act*

17. Social Services (continued)

Other items affecting the management of personal information include the Department's Information Technology Security Manual, Information Technology Security Policy Document, Social Services Staff Orientation Manual and various other policies and procedures within Social Services.

Community Living Division

The Community Living Division of Social Services provides programs and services for persons with intellectual disabilities and their families. These services are delivered in the community and in the Valley View Centre in Moose Jaw, a residential home for persons with intellectual disabilities. Support services focus on case management, therapy support, family support and community-based services.

Personal information regarding clients is collected and used in order to plan and deliver services. Personal information is shared with other divisions within Social Services including the Income Security Division and the Child and Family Services Division. Personal information is shared with other government agencies or departments including Learning, Health, and Justice with the consent of the client and/or family. In addition personal information is shared with Regional Health Authorities, external physicians, and Community Based Organizations (CBOs) with client and/or family consent.

Community Living collects personal information for the Public Trustee and the Department of Indian Affairs. It is important to note that with many of Community Living's clients, they may not have the intellectual ability to consent to the provision and use of personal information. Therefore, in many instances consent is obtained from family members.

Career and Employment Services Division

The Career and Employment Services Division of Social Services is responsible for a number of programs including the Provincial Training Allowance, Student Financial Assistance, Family Literacy, Career and Employment Services and Work-Based Training for the Unemployed. Saskatchewan Learning administers these programs.

Personal information is collected in order to operate these programs. Personal information collected includes name, address, phone number, e-mail, date of birth, gender, SIN, Health Services Number, Marital Status, Drivers License Number and Class, Citizenship, Education History, Employment History, Social Assistance Recipient Status, Language of Service and Intervention, Family Type, Disability Status, Visible Minority Status, Number of Dependants,

17. Social Services (continued)

Aboriginal Status, Treaty #, Band Affiliation, and the Date the Individual signs the Registration Form at Career and Employment Services for the release and use of information.

Information collected by the Division is also collected, with consent, on behalf of the Government of Canada for EI eligible clients in receipt of programs and services delivered by the Province under the authority of the Canada-Saskatchewan Labour Market Development Agreement (“LMDA”) and in turn the Government of Canada shares personal information with the Division to determine client eligibility for programs delivered under the LMDA.

The Division also shares information with the Income Security Division for shared clients. The Client Registration Form, which requests the personal information listed above, was developed as the standard in the Division to define what is personal information.

In addition to Department policies and procedures, legislation and the LMDA, the Career and Employment Services Division’s management of personal information is governed by the Employability Assistance for Disabled Persons Agreement with the Department of Learning, which provides for the sharing of information between the two Departments in order to fulfill each Department’s mandate.

Housing Services Division

The Housing Services Division provides a variety of housing assistance programs. Personal information is obtained and disclosed for the purposes of determining eligibility for housing assistance and participation in various housing programs.

Information obtained includes family information such as name, address, telephone number, family composition, birth dates as well as information specifically needed for program delivery including insurance information, financial information, medical information, tenant information, etc.

Information is collected and shared with CMHC in regards to mortgage/loan programs and repair and grant programs, Aon Reed Stenhouse Inc., Social Housing’s insurance broker, and Housing Authorities. Information is also shared with other divisions within the department (i.e. Social Assistance Program staff for common clients) and other government agencies or departments outside Social Services (i.e. SaskPower, SaskEnergy, etc.). Clients provide consent to this sharing of information when they apply for the various housing assistance programs.

17. Social Services (continued)

The Division considers any information about a client to be personal information. In addition to legislation, program requirements affect how the Division manages personal information.

Housing Program Development is a research branch of the Housing Services Division. Housing Program Development carries out surveys of clients living in Social Housing units. The information collected is anonymous and once survey information, which may contain client names and/or addresses, which are temporarily used for follow up in gathering data, is inputted, the surveys are destroyed so that no record of individual personal information is maintained.

Information needs for program evaluations are used to determine what personal information should be gathered. Prior to conducting a survey the questionnaire goes through a review process. The information gathered is generally demographic and income in nature, similar to Statistics Canada surveys.

Any surveys conducted are sent to clients with a covering letter explaining the nature of the survey and why the survey is being conducted. Participation is voluntary. The results are only used internally and are not shared with third parties.

Child and Family Services Division

The Child and Family Services Division is responsible for a number of programs and services for children and families. The main program and service areas are Child Protection, Family Support Services, Targeted Support Services, Children's Services and Adoption Services.

The primary purpose of Child Protection Services is to identify children who are in need of protection due to child abuse or neglect. Reports that a child may be abused or neglected are investigated and, if required, action is taken to ensure child safety. Family Support Services include a range of in-home services to provide support and to assist families to help resolve child safety issues so that out of home placements can be avoided and to promote and facilitate healthy family living.

Services are provided by agreement with parents, and may be provided by department workers or purchased directly from professionals, private individuals and community-based agencies. Family Support Services include providing a family with a parent aide or homemaker on an intensive, short-term basis; providing instruction and training in basic life skills, nutrition, hygiene, etc.; offering parenting education; conducting assessments; and providing counselling.

17. Social Services (continued)

Targeted Support Services include programs and initiatives, which are voluntary and are intended to prevent families who have identified problems from requiring a more intrusive intervention. Programs include the Teen and Young Parent Program, which provides various counselling and support services to pregnant and parenting teens and Family Violence Services Programs, which are designed to help eliminate family violence.

Children's Services provides a number of resources available to children and youth who must be removed from their families on either a temporary or permanent basis, with the primary resource being foster homes. Adoption Services provide a variety of legal processes by which a child can be adopted.

Information on children, youth and families is gathered under *The Child and Family Services Act* where there is reason to believe that a child may be in need of protection. Information is gathered for the purposes of conducting investigations into abuse and/or neglect of children, providing services to families to intervene where abuse and/or neglect has been substantiated, and for providing services to children who may need to be removed from their parental home and placed in out-of-home arrangements. Section 74 of this Act stipulates when, how and with whom information gathered can be disclosed.

The Adoption Program collects personal information for the purposes of adoption. It is used and disclosed in the adoption process with the consent of the persons involved. (The Minister acts on behalf of the child as legal guardian).

All information gathered is personal and includes addresses, family composition, medical, social, emotional, and environment information, vital statistics, home standards information, CPIC and case notes information.

The Division collects information on behalf of other levels of government and shares information with other levels of government. Information may be collected as per interprovincial protocols. At times, Saskatchewan may be asked to complete a home study of a Saskatchewan family on behalf of another provincial child protection agency.

The Adoption Program interacts with other provincial departments in Canada and may collect information regarding requests in the adoption and post adoption program. An interprovincial protocol is established and consent is required in all matters except for Post Adoption services where a person may initiate a search for their birth parents and/or birth family members. The personal information collected for the search is not released without the consent of the individual(s) involved (i.e., the birth parents or family members).

17. Social Services (continued)

The interprovincial protocol (established with a national consultation committee including Justice) allows for provinces to request information from each other through existing search mechanisms to assist in locating a person who is the subject of the search.

The Division shares information between other Social Services divisions if there are mutual clients and it is deemed necessary to carry out a mandate. The Adoption Program shares personal information within groups or sections of Social Services only when it is determined that the information shared is in the best interests of the child. Once the adoption is finalized in court, the file is placed in the legal adoption vault and this information is no longer shared within the Department.

In the course of providing services to children at risk and their families, it may be necessary to share information relevant to joint work on behalf of children, youth and families with other government departments and agencies as follows:

- Justice/Private lawyers - to represent the Department at Family Services Hearings
- Mental Health services - referral and coordination of services
- Schools - to plan for children's educational needs and/or to advocate for the child with the school system and at times, it may be necessary to move children from their school setting once they are admitted to the care of the Department
- CBOs - referral and coordination of services
- Police - to conduct joint investigations
- First Nation Child and Family Services Agencies
- INAC
- Health - registration for health coverage while child is in care
- The Adoption Program also interacts with Health (Health Registration, Public Health re immunization records of adopted children), Justice (for consultation on complicated matters that may concern birth parents, adoptees and adoptive applicants/parents)

Sharing information with consent occurs, on occasion, with Christian Counselling Services in Saskatoon who also deliver adoption services. The one exception where information is shared without consent is when Christian Counselling Services request a search with Social Services records to determine whether any of their adoptive applicants have had child protection involvement with the department. If the adoptive applicants have had involvement, the Department will confirm there has been involvement.

17. Social Services (continued)

The Post Adoption Registry within the Adoption Program will contact other government departments or agencies in a search for an individual; however, other than the name and birth date of the individual, personal information is not released. Once the personal information is collected, it is not released from the department without consent.

The Post Adoption Registry provides information to the Department of Indian Affairs in Ottawa confirming whether the adoptee has Treaty Status according to Social Services' records. (Consent has been provided.)

The Adoption Program may share information regarding a child who is being considered or prepared for adoption with a First Nations Child and Family Services Agency.

In the course of conducting investigations and for the provision of services, it is necessary to gather information from the above noted systems (Health, Education, FNCFS, etc.) to assist in making a determination of a child's safety and in the provision of ongoing services to reduce the risks to the child's safety. Criminal Records information is received from police authorities for those pursuing a home study.

The Post Adoption Registry within the Adoption Program receives information from other government departments and agencies as follows:

- The Department of Health confirming the name and birth date of the individual as well as whether the person who is searched for is alive or deceased and resides in Saskatchewan.
- The Vital Statistics Division within the Department of Health confirming birth, marriage or death documents. Consent is required prior to release of Live Birth Registration unless the adoption occurred after April 1, 1997. With any adoptions occurring after this date, the Department has the authority pursuant to *The Adoption Act* to release to the adopted adult or birth parent, the Live Birth Registration form, unless the party requests a veto forbidding release.
- Information regarding a search for an individual from Post Adoption Registries in other provinces operated by the Ministry.

The Adoption Program may receive personal information from Christian Counselling Services Agency in Saskatoon who also deliver adoption services, however, this information is only released with the consent of the individual involved. In addition, the Adoption Program may receive information from a First Nations Child and Family Services Agency regarding a child being considered or prepared for adoption; or regarding First Nations adoptive applicants who have applied for adoption (consent required with adoptive applicants).

17. Social Services (continued)

Assessments completed on children from professionals such as Child and Youth, Early Childhood Intervention Program and educational assessments are received from other departments or agencies and disclosed to adoptive applicants who are seriously considering accepting the child into their family as an adoption placement. If they do not accept the child for adoption, the information is returned.

The division considers all information collected regarding any Social Services client to be personal and confidential information. Section 74 of *The Child and Family Services Act* provides the parameters for sharing information gathered for the purposes of the Act. This includes information that the Department is given that had been gathered through other legislative mandates such as Young Offenders, Health information or Criminal Code investigations.

Other information requirements aside from legislation affecting the Division's management of information include the requirement to make payments on behalf of children, youth and families through the Family & Youth Automated Payment System (FYAP), requests for Special Allowance made to Revenue Canada (Canada Customs and Revenue Agency - CCRA) and notifications sent to INAC for the purposes of cost sharing with the Federal Government.

Income Security Division

At the Income Security Division, personal client information is collected and used to determine eligibility for Income Support programs. Included are the Saskatchewan Income Plan, the Social Assistance program, the Child Daycare Licensing and Subsidy programs, the Saskatchewan Employment Supplement, the Saskatchewan Child Benefit and the Benefit Adjustment.

Personal information is documented on the program application form. Personal client information is disclosed where client consent exists and/or where the authority is provided for in either legislation for *FOI* for the purposes of requesting further information electronically such as CPP/EI/WCB, to provide a unique client identifier for case conferencing and/or for determining ongoing eligibility for benefits and services.

The Income Security Division does not collect personal information on behalf of another department, agency or level of government.

The Income Security Division shares information within the organization where the client has more than one involvement and the information is required to determine case plans or eligibility for services (example, a family services' involvement and Social Assistance involvement).

17. Social Services (continued)

The Income Security Division shares information on mutual clients with the Salvation Army, other government departments such as Northern Affairs, the Public Trustee, the Maintenance Enforcement Office (Justice), and other provincial Social Services' Departments for the purposes of verifying eligibility for benefits, and preventing duplication of benefits.

The Income Security Division receives information from CCRA to determine eligibility for the Saskatchewan Child Benefit and the Benefit Adjustment programs. Client information is received from Human Resources Canada for the Old Age Security/Guaranteed Income Supplement programs to determine eligibility for the Saskatchewan Income Plan program. In addition, the Division also receives information from CCRA for post verification purposes for both the Social Assistance and Saskatchewan Employment Supplement programs.

The Income Security Division defines personal information as defined by *the Freedom of Information and the Protection of Privacy Act (The FOI Act)*. *The FOI Act* governs the division with respect to personal information. Aside from this legislation, interdepartmental/inter-agency agreements and memorandums of understanding also affect the division's management of personal information.

Property Management Branch

The Property Management Branch of Social Services is responsible for co-coordinating and supporting all Social Services programs in the areas of capital projects, construction and tenant improvements, the procurement of capital assets and office supplies, records and forms management, print procurement, mail services and vehicle and asset management.

Property Management is responsible for managing the services necessary to support the day-to-day operations of Social Services. Property Management does not have any direct client contact other than the occasional client calling regarding or dropping off *FOI* applications, which are the responsibility of Property Management.

Because Property Management is responsible for managing *FOI* requests, it shares information with other departments within Social Services. All client information is considered personal information.

Research and Evaluation Division

The Research and Evaluation Division of the Department of Social Services helps the Department design, implement and assess the effectiveness of programs and policies. The Division also provides basic research services to the Department, including analysis of social, demographic and economic trends.

17. Social Services (continued)

The Division will also conduct special studies. In carrying out its mandate the Research and Evaluation Division will use personal information collected by Social Services, as well as other government agencies or departments, in conducting research on program trends.

Financial Management Division

The Financial Management Division of Social Services is responsible for co-coordinating and supporting all program areas in the program divisions in the areas of budgeting, forecasting, financial planning, financial reporting, financial management, payment processing, payroll and collection of overpayments for inactive Social Assistance Plan (SAP) and Saskatchewan Employment Supplement (SES) files. As a provider of central support services this Division has little front line contact with clients with the exception of collection of payments. In the process of making payments the Division generates details on payment information on Foster Children using information collected by front line services. In collection activities personal information is provided to collection agencies under Section 16(h.1) of *The FOI Act*. When audits are conducted, child protection case files are reviewed to support payment activities.

Technical Services Division

The Technical Services Division of Social Services is responsible for providing support services to other divisions within the department, primarily in the area of repair work. Technical Services does not collect personal information, however the Division does use personal information to conduct inspections of repair work.

For purposes of program delivery and administration, personal information is shared with housing authorities, delivery agents, Financial Management Division of Social Services, Legal Services and divisions responsible for various repair programs. In addition to these other departments and agencies, Technical Services receives personal information from Saskatchewan Justice, Consumer Protection for purposes of conducting inspections.

Information and Technology Services

Information and Technology Services does not collect, use or disclose personal information in the course of business activities, collect personal information on behalf of another department, agency or level of government, share personal information with other groups or sections within the organization, other government departments or agencies, or receive personal information from another department, agency or level of government. They facilitate sharing for program areas.

17. Social Services (continued)

ACCOUNTABILITY

The Social Services' FOI Administrative Coordinator, whose identity is made known to the public, has overall responsibility for managing the policies and procedures regarding personal information and is responsible for overseeing compliance with them. His primary responsibilities include records management, forms management and print procurement, FOI and HIPA Officer duties, security management, and mail management.

The Coordinator, Legal Services is involved in establishing and maintaining legal policies and procedures related to personal information.

In the Child and Family Services Division central program managers and regional office directors are accountable for managing policies regarding personal information. The identity of these individuals is made known to the public.

The Department does outsource processing (IT or otherwise) of its personal information. They have a Facilities Management agreement with ISM Canada under which it operates and supports the mainframe and midrange computing environments. The Department's major applications, which are run on the processors housed at ISM's facility at the University of Regina campus, include the Client Index, Saskatchewan Assistance Plan, Child Care Subsidy, Saskatchewan Child Benefit, Saskatchewan Employment Supplement, and the Family and Youth Automated Payment systems. Schedule "D" of the Facilities Management agreement outlines the roles involved in security of the parts of both ISM Canada and Saskatchewan Social Services with respect to the protection of information in third party care. Further details can be found in the IBM Global Services document GSD-331 (Information Security Controls for Saskatchewan Services).

The Child and Family Services Division outsourced the electronic imaging of its adoption files in 2001 to a private company. At times the Division contracts with research companies for research projects. Personal information is released to these contractors with specific trust conditions that they agree to within the contract.

Social Services has general policy and procedures manuals that affect the Department's overall management of personal information. These policies include Sensitive Mail Handling and Destruction of Confidential Information policies. Compliance with destruction of confidential information policies is performed as part of an annual audit. On-going staff training helps ensure compliance with Sensitive Mail Handling policies.

17. Social Services (continued)

Information and Technology Services recently developed procedures where all staff are made aware of, and required to sign off on, a policy regarding personal information. To monitor compliance with the policies mentioned above, ITS uses some system password enforcements.

The Community Living Division has a review policy in place in regards to Approved Private Service Home (APSH) service providers to deal with complaints or inquiries regarding APSHs.

Valley View Centre, which is part of Community Living, follows Social Services general policies and procedures in regards to personal information but also has its own policies and procedures around personal information, especially related to the Centre's Resident Information Tracking System. These policies and procedures are based on the guidelines of the *HIPA*.

The library at the Centre has a complete set of Centre's policies and procedures manuals, which can be viewed by the public. The Centre has communicated its policies and procedures to staff and most recently in May 2002 the director of the Centre prepared a memo to staff on Confidential Client Information, which was reviewed as part of the training all staff participated in during June 2002 regarding personal information. Any complaints regarding policies and procedures are directed to the Minister of Social Services office for review and follow up.

In addition to Social Services general policies and procedures relating to personal information, Housing Services staff must follow the Division's Mortgage/Loans Procedure Manual. In order to protect personal information in their possession, housing authorities are required to abide by the confidentiality policy statement set out in the Saskatchewan Housing Authority Policy and Procedures Manual.

Child and Family Services has its own Children's Services Manual and Family Centred Case Management and Adoption Manuals, in addition to Social Services' general policy and procedures manuals. The Children's Services Manual was updated in June 2002. The Family Centred Case Management and Adoption Manuals are currently being updated. The update review process indicates that there is need to confirm the policy regarding the process that individuals use to gain access to their own information, review the method by which information is provided to custody and access assessors, and bring more clarity to the process by which information is shared interprovincially.

17. Social Services (continued)

The Income Security Division's policy with respect to personal information is contained in the Social Assistance Policy Manual, which is available to the public. These policies were last updated in June 2002. The policies around client confidentiality are contained in the Orientation manual received by new employees and were most recently communicated to all existing staff in June 2002.

The Research and Evaluation Branch performs ethics reviews on new research proposals to help ensure that personal information is protected. Before consent is given to proceed with a new research study, the researchers must comply with any specific conditions laid out regarding the protection of information.

Information and Technology Services has written policies or procedures with respect to personal information in their possession. The procedure regards restricted access involvements (internal service only). This procedure is not available to the public and was last updated in 1999. The Division has communicated the policies to all employees so that they are fully aware of their obligations.

Social Services reports that regional managers, program managers, supervisors, local experts and central office program managers received *HIPA* and *FOI* orientation in January and February 2002. It is reported that all staff have been involved in unit reviews of legislation, policies and procedures related to client confidentiality in June 2002. With respect to inquiries and complaints, *FOI* inquiry procedures have been established. Complaints and/or inquiries are directed to management. The client also has the option of contacting the Privacy Commissioner directly.

Complaints and enquires regarding the Career and Employment Services Division are normally handled by the Minister or Deputy Minister's office. A Referral System is used to record and track any complaints or enquiries and the responses.

In the Housing Services Division, inquiries and complaints regarding the Division's handling of personal information are referred to the administrator or supervisor for the area or to the Coordinator, Legal Services.

The Child and Family Services Division has a process in place for the handling of complaints and inquiries. The process is outlined in a brochure "Your Right to Appeal". The policy is to provide this brochure and information to all families who will be receiving child protection services from the Department.

17. Social Services (continued)

Child and Family Services monitors compliance with its policies and procedures by reviewing any complaints regarding possible breaches of confidentiality. In addition the Division has recently hired a Quality Performance and Improvement/Accountability professional whose role will be to oversee compliance with all policies within Child and Family Services. Meetings are also held with client representatives including Saskatchewan Youth In Care and Custody Network, Saskatchewan Foster Families Association who may report on non-compliance to policies and procedures.

In order to monitor compliance with the policies related to personal information at Career and Employment Services, Division managers routinely conduct random audits to review individual case files for compliance.

At the Income Security Division, to monitor compliance with the above policies and procedures, program staff are trained in the program area prior to dealing with the public, sign an oath of office, and where required, use of personal information is monitored through system tracking reports, and coaching through supervision.

IDENTIFYING PURPOSES

The Data Quality Committee (DQC), comprised of officials from business areas covered by the One Client Service Model (OCSM), was established to oversee the collection of information required from each program area in the Department. The Committee's mandate is to develop standards and processes and ensure data integrity. Officials with knowledge and expertise from the different Divisions are part of the DQC.

The Community Living Division determines what personal information to collect based on planning with client service providers. Individuals are informed as to why personal information is being collected and how it will be used during intake meetings and at subsequent meetings with the client.

The Valley View Centre classifies the personal information it collects according to the type of information and its sensitivity. The Centre's process for doing this is meant to follow *HIPA*. The most sensitive personal information at the Centre is considered to be the health information of its clients. This information is kept in a locked area in the Health Records Library at the Centre and is only accessible through the Centre's Health Records Technicians. Access to electronic information is on a need to know basis and is very restricted. This general rule applies to all divisions of Social Services.

17. Social Services (continued)

At Career and Employment Services, career information officers and employment consultants work with clients to develop work action plans and as part of that process the clients are explained the information requirements and how that information will be used. Managers in the Division are responsible to work with new staff to ensure the proper handling of personal information, especially during the probationary period.

Prior to designing program application forms the Housing Services Division determines what information will be required to deliver a certain program. Regarding insurance applications, Housing Services collects information based on instructions from Aon Reed Stenhouse Inc., the Division's insurance broker. Applicants for housing assistance are advised verbally as to why their personal information is being collected and how it will be used. Standard application forms state that information provided is confidential and the client gives written authorization to use and share the information.

Legislation, policies and procedures outline what information Child and Family Services requires for investigation purposes and what is necessary to make assessments and provide appropriate interventions with families. The Division's Adoption Program dictates what personal information is collected for the purposes of adoption. Due to the nature of the services provided by the Child and Family Services Division all information is treated as highly confidential. All information collected is maintained in a client paper file. Information is also maintained in computer files. Access to electronic files is restricted by user and password protection is in place.

Adoption files are considered to be very confidential. When the adoption is finalized the paper file is placed in a secure place and the file is electronically imaged and only accessed by Central Post Adoption Registry employees. Assisted Adoption files are maintained in the region. Prior to electronic file closure, the information is sent to the Post Adoption Registry to be placed on the legal adoption file. Adoption files that do not proceed to an adoption placement are stored as deadwood in file rooms in department offices and are scheduled for destruction as per policy in place (10 years after last involvement with the department).

The Income Security Division uses program legislation to determine what personal information they maintain. The Division does not classify the personal information they collect according to sensitivity. All client information required for program delivery is considered sensitive.

17. Social Services (continued)

The Financial Management Division uses the province's Financial Administration Manual, which sets out the personal information required to support a payment.

Various divisions of Social Services, which deliver services to clients, create personal profiles by combining personal information from various sources in order to effectively and efficiently deliver client services. Child and Family Services, as an example, will create personal profiles by combining personal information from various sources in order to make up a family assessment. Electronically, the Division combines all of a client's involvements into one profile on ACI (Automated Client Index).

The Data Quality Committee oversees new development and considers the implications for all business areas using the One Client Service Model. In general when Social Services is implementing a new technology or system, Social Services existing e-mail and WEB Usage policies are to be followed. Social Services does not have any confidential client data available on the Internet and FTP (File Transfer Protocol) data exchanged with outside agencies is encrypted before being sent over the Internet.

Prior to implementing a new process at the Income Security Division, the Department ensures what electronic data is secure. Where data is shared with another organization a memorandum of understanding or agreement is signed identifying why the information is needed, the use for the information as well as ensuring that it is essential for their program operations.

Prior to implementing a new business process reliant on the collection and use of personal information the Child and Family Services Division assess the personal information related risks. As an example, the Adoption Program has been working closely with the Department of Health regarding implementation of information (i.e. *HIPA: Health Information Privacy Act*). The Post Adoption File Imaging Project was undertaken with the utmost sensitivity and concern regarding the handling of personal information. The intent of the electronic imaging is to preserve the adoption information indefinitely on file. The paper file was at risk for fire and water damage etc.

In general, applicants for Social Services programs are advised in advance why and how their information will be used through the applicable signed consent and release process. Social Services front line staff are trained in their program area prior to dealing with clients or the public and are made aware of both the program rules and client consent. The Oath of Office is taken at the start of employment.

17. Social Services (continued)

In the Child and Family Services Division individuals are not always told why their personal information is being collected and how it is going to be used. Caseworkers are required to identify themselves to clients and the purpose of their involvement when they meet with a client. However, collateral contacts are often made for the purpose of investigating a child protection referral and the family may not be aware that their personal information is being gathered. *The Child and Family Services Act* provides authority for this type of collateral contact to occur. Once contact is made with a family, caseworkers by policy are responsible to include families in all further assessments and planning.

In the Child and Family Service's Adoption program, all individuals understand the reason why their personal information is collected and how it will be used for the purposes of an adoption. This is accomplished in the intake meeting and ongoing meetings and services provided. In Post Adoption services where searches are conducted for the purposes of reunions with adoptees and birth parents, one of the parties is not aware they are searched for until their identity and location are confirmed. The personal information about the case is not released if the person being sought and located does not want to be involved and written consent is not provided.

At the Research and Evaluation Branch if new information is collected as part of a research project, individuals are informed by letter and by an interviewer as to why their personal information is being collected and how it is to be used. Consent must be informed and voluntary before the information can be collected and used. Individuals collecting the information receive training with every research project.

In Child and Family Services all staff are trained in Family Centred Case Management and the Children's Services Approach as well as the legislation. This training speaks to what information is needed to do an assessment and planning. Employees in Child and Family Services are required to hold a Bachelor of Social Work. Social Workers are trained in the Code of Ethics for Social Workers and the importance of maintaining personal information confidential.

CONSENT

In general the various divisions of Social Services gain consent from individuals regarding the collection and use of personal information. Child and Family Services is the exception to this, as discussed below.

17. Social Services (continued)

The Community Living Division gains consent from individuals at the time information is being gathered from the client. Consent forms are used to record consent and are kept on file. Valley View Centre management are currently addressing the issue of monitoring the use of personal information in accordance with the draft *HIPA*. Valley View Centre will disclose medical information to third party health care providers in accordance with the draft *HIPA*.

The Career and Employment Services Division gains consent from clients as part of the Standard Registration and Release Form, which is signed by the client. The date of the signed consent is recorded in the Career and Employment Information System. The Standard Registration and Release Form authorizes the Division to share personal information with third parties. Information is shared with educational institutions or other agencies involved in the implementation of a client's return to work action plan.

Data related to clients is used for evaluation purposes as well. Any evaluations external to government are given data either in aggregated form (no personal identification) or, if when personal identification is involved (e.g., surveying), the external evaluator is contracted through RFP with stringent guidelines for data management and date purge as well as overall adherence to Canadian Evaluation Society Standards for Ethical Practice.

Housing Services obtains consent through standard wording on its program application forms, which must be signed by the client. Application forms are kept on file, which provides a record of consent.

Child and Family Services do not always gain consent from individuals regarding the collection and use of personal information. In the Child Protection program, consent to collect personal information is not required as legislation allows staff to gather information for the purposes of determining a child's safety. Foster parents sign a consent and release of information form during the home study process. In the Adoption Program individuals sign off on personal information gathered or they provide specific written consent. Regarding searches conducted in post adoption, personal information gained (names and birth dates mostly) are not released without the consent of the individual involved. In Post Adoption Services consent is recorded on departmental forms for services such as search and reunion and release of Birth Registration documents. In Child and Family Services users of personal information view the written consent on forms and documents on file to ensure the personal information can be used and/or released as authorized.

17. Social Services (continued)

Child and Family Services ensures that the use of personal information is only in accordance with the consent obtained and governing legislation through training and ongoing supervision. In addition the Division's Quality Assurance measures monitor compliance. Meetings with client representatives including Saskatchewan Youth In Care and Custody Network and the Saskatchewan Foster Families Association help ensure the proper use of personal information.

Child and Family Services will not always inform individuals and gain their consent prior to releasing information to third parties. At times, Section 74 of *The Child and Family Services Act* is utilized to disclose information. In the Adoption program, consent is gained prior to releasing information except for circumstances in post adoption when a doctor writes on behalf of an adoptee requesting medical information in background history because of serious health concerns. Only non-identifying information is provided.

The Income Security Division always gains consent from individuals prior to the collection of their personal information. Client consent is generally obtained on a paper program application form. Where the applicant goes through a call center, the consent is initially verbal and is recorded on tape and then followed up by a signed consent.

The information is valid for the length of time a client is on the program and is intended to cover all purposes for which it is used.

In the Income Security Division, users of personal information are informed of the specific consent through program requirements, MOUs, and client consent. In order to ensure that the personal information obtained is used only in accordance with the consent obtained at the Income Security Division, program staff are trained in the program area prior to dealing with the public, sign an oath of office, and where required, use of personal information is monitored through system tracking reports.

The Income Security Division does inform individuals and gain their consent prior to disclosing their personal information to any third party. Clients are informed of program requirements around the release and need to request personal information through the signed consent form.

For research projects being conducted by the Research and Evaluation Branch consent to collect and use personal information is obtained by letter and verbally when the information is being gathered verbally. Consent is recorded on an informed consent form.

The Financial Management Division will advise a client either verbally or in writing prior to sending their outstanding account to a collection agency.

17. Social Services (continued)

For all departments, access to personal information is restricted to staff who need access to it to help ensure that the personal information collected is only used for the purpose it was intended.

The Data Quality Committee conducts monitors and runs reports to check for issues regarding the unauthorized use of personal information. At the Career and Employment Services Division program audits have also been conducted and included client contact and discussions. Managers also routinely conduct random audits.

LIMITING COLLECTION

In general Social Services uses standard client program application/registration and release forms to ensure that only information needed to administer the specific program or service is requested. Standard policies and procedures and training ensure that when recording data, only the relevant information is included. The collection of personal information is based on the needs identified by the client service providers.

Social Services social workers are bound by professional standards (Canadian Association of Social Workers Code of Ethics) and Social Services policies and procedures to only use personal information for the purposes it was collected.

In order to ensure that only the required personal information is collected by the Research and Evaluation Branch, data collection goes through several revisions and committee processes before data collection actually starts for a new research project.

LIMITING USE, DISCLOSURE, COLLECTION & RETENTION

To ensure that personal information is only used for the purpose it was collected the Department recently provided training and awareness sessions on this issue to all staff in June 2002. Department policy and procedures manuals indicate how personal information can be used and disclosed. Management in the various divisions will conduct random audits of case files to identify any issues including management of personal information issues.

In general, the various divisions of Social Services follow the Department's general policies regarding retention and disposal of records. Housing program files are retained and disposed of in accordance with the Saskatchewan Housing Corporation retention schedules. Paper documents are shredded in accordance with Social Service's Destruction of Confidential Information policy. Electronic data stored on surplus hard drives are erased using software provided by SPMC Security Services. Non-operable hard drives are removed and physically destroyed.

17. Social Services (continued)

Due to the physical and mental health condition of its clients the Valley View Centre will collect personal information about a client from sources other than the client including family member and the assigned social case worker(s).

Consultants in the Career and Employment Services Division will receive information from training institutions (i.e. SIAST) on a client's progress or attendance in a program when financial sponsorship has been provided. This information is within the scope of the Standard Release Form obtained by the Division for each client.

Housing Services will collect personal information from credit bureaus and lending institutions as well as rental references supplied on application forms. This information is within the scope of authorization obtained from the client as part of the standard application process.

In the Child and Family Services Division there is "umbrella" legislation (section 74 of *The Child and Family Services Act*) that allows the sharing of information only to carry out the intent of the Act.

Child and Family Services will collect personal information about an individual from third parties. As previously noted legislation governing the Division allows staff to make collateral contacts when conducting child protection investigations or when assessing a child in care. Personal information may be obtained from Health, Education, Band offices, and private counselors, etc.

The Income Security Division collects personal information about an individual from third parties. The Saskatchewan Employment Supplement (SES) program derives CPP/EI/WCB and support information directly from the source. As well, the family composition is derived from Saskatchewan Health. Both the Saskatchewan Assistance

Plan (SAP) and SES programs collect tax information from CCRA for the purpose of income matching verification and several like matches are completed with other organizations for program verification.

MAINTAINING ACCURACY

The Data Quality Committee oversees the maintenance of accurate personal information and has in place reporting that identifies issues. If the Committee discovers some information discrepancies, appropriate corrective action is undertaken. Through the integration of Information Systems with other agencies such as the Government of Canada, information can be verified and/or corrected. The Department is also subject to the Provincial Auditor's annual audit.

17. Social Services (continued)

In general, as long as a client's file is open and active, the information is kept up to date. Once a file is closed or becomes inactive the information will no longer be kept up to date. Most information is obtained through front-line staff contact with clients. Child and Family Services will also obtain information from client family members and collateral contacts.

To further ensure accuracy of information the Income Security Division conducts internal audits of program administration, verification processes, schedules regular program matching to verify data, and requests hard copy documentation.

At the Valley View Centre formal Care Planning meetings are conducted every two years for its clients and at that time a formal review of the individual's personal information is completed to ensure that the personal information is accurate.

Housing Services performs an annual review of client information and updates it as required as well as updating application information every 6 months.

SAFEGUARDS

Social Services has safeguards in place to protect personal information from unauthorized access, disclosure, copying, use or modification. Staff are assigned to organizational roles and functions and are limited in their access to both electronic and paper copy information on a need to know basis. If staff attempt to access electronic data that is not part of their user profile, a reason for access is required from their supervisor and is logged prior to changing their user profile. In the Income Security Division clients personally known to staff will have their data access restricted.

Canadian Police Information Centre (CPIC) searches are performed on all new Social Services staff prior to being hired to help protect personal information of clients and the clients themselves.

Physical security measures in place to protect personal information include restricted key/card access to facilities after hours, locking filing cabinets, locking shredding/paper disposal boxes, privacy glass in most reception areas, sound proofing in interview rooms, panic buttons in interview rooms, unican (combination) locks in certain highly restricted areas and clean desk policies in certain offices that deal with sensitive client information. Computer server rooms are locked. Access to mainframe and midrange computer facilities are controlled under a Facilities Management Agreement.

17. Social Services (continued)

Social Services requires that employees, contractors, partners and any other third parties with whom personal information is shared sign confidentiality agreements. In general, no outside organizations have access to Social Services systems without a legal contract, which contain confidentiality wording. Those that do have access cannot access the Social Services' personal information through the Internet. All applications are password protected and can only be accessed through Social Services LAN. Internal networks are protected by firewalls. Encryption is employed for all data exchanged with outside agencies over the Internet.

In general Social Services does not actively monitor third parties' compliance with confidentiality requirements. The exception is the Community Living Division, which enters into agreements with Community Based Organizations (CBOs) that contain clauses regarding the confidentiality of personal information. CBOs compliance with the agreements is monitored through Community Living's Basic Standards Review process.

Social Services is committed to participate in the Security Charter initiated by the ITO whose purpose is to develop Security Policies for the Government of Saskatchewan.

With regards to the Provincial Auditor's Fall 1999 Report on Information Security the following areas still need to be addressed by Social Services:

- The Provincial Auditor recommended that agencies assign the responsibility of IT security to a senior manager who is independent of IT operations. To date Social Services has not formally assigned responsibility to such an individual. The Information Management Governance Council has been formed and responsibility will be one of the issues to be addressed by the Council.
- The Provincial Auditor recommended that the security administrator(s) report directly to the senior manager responsible for IT security. To date this had not been formally done. The Information Management Governance Council will be addressing this issue.

OPENNESS

Social Services makes its policies available to the public upon request. Certain program policies, such as the Social Assistance Plan policy manual are available on the Internet. The Department also makes brochures available to the general public regarding a person's right to request personal information.

17. Social Services (continued)

PROVIDING ACCESS

In general Social Services allows individuals access to their personal information, providing the identity of the individual has been ascertained, as permitted under *The FOI Act*, the *Child and Family Services Act*, the *Adoption Act* and the Department's Social Assistance Plan Manual. When personal information is released to an individual the general process is to record the information released, the name of the recipient and the release date.

Personal information is not released to third parties without written consent of the individual unless otherwise permitted under *The FOI Act*. If the authority to release information is unclear the FOI Coordinator and/or the Coordinator, Legal Services becomes involved. The recipient of personal information is only bound to adhere to the Department's privacy policies if they are a service provider under contract with the Department.

The process for responding to *FOI* requests is that identified in *The FOI Act*. All *FOI* applications and responses are kept in the FOI Admin Coordinator's files. The file includes the applicant's name, date received, date response released, individual that prepared the response, nature of the response and if the response is not too great, an actual copy of the response.

At the Valley View Centre access to personal information is very limited due to the functional ability of the clients at the Centre. The Centre will allow clients to review their personal information in the presence of a Health Records Technician. If the release of personal information at the Centre is unclear, the FOI Coordinator is contacted and provides advice on the release of information.

Child and Family Services generally has four different situations where personal information may be shared as follows:

1. Requests from Federal Crown or lawyer

These requests are accompanied by a Consent to Release form signed by the client allowing the Department to disclose the personal information to the lawyer(s). Generally all Social Services information is requested - these are usually in response to Residential School Claims or other claims where Social Services is not a defendant. Requests are given to one central staff person who coordinates the disclosure. The central staff person makes a request to the regional office for the file(s). A letter is sent to the requester acknowledging receipt of the request and explaining the procedures.

17. Social Services (continued)

If Income Security files are requested as well, a staff person is copied on the letter to let them know to request their files as well. Once received, the files are photocopied - two copies are made - one for Child and Family Services' records that remains unedited and one that is edited for disclosure purposes. All references to third parties are obliterated from the file in accordance with Child and Family Services' guidelines. The edited file material is forwarded to Justice to ensure editing is acceptable. The information is forwarded from Justice with trust conditions to the lawyer for the requester. The original file is returned to the regional office. The original request for information and all other correspondence regarding the request is kept in central filing. This would include information regarding when the request was received and when the information was shared.

2. Non-litigation requests for information

These requests are usually made by the client directly to the regional office. The practice varies from region to region as to what is disclosed but generally the disclosure follows the following steps. The requests are made to the Regional Director or Program Manager of the regional office. At times, the file material is summarized into a brief document and presented to the individual. This is especially true if the file is very large and would be quite time consuming to review. Other times, a staff person would sit down with the requester while the file is reviewed. All references to third parties must be removed prior to sharing the file. File material is not handed over to the requester.

3. Statements of Claim where the Social Services is a defendant

All relevant file information is shared with the plaintiff (usually former clients) through their lawyers. The Disclosure of documents is done by way of Statement as to Documents. The procedures are as follows. When a statement of claim is received by Child and Family Services it is forwarded to the Manager of Litigation Support who handles the remaining steps. All file material pertaining to the plaintiff is requested from the regional office or other location. Often in cases of historical abuse claims, the file is in central storage or in archives if it has not yet been destroyed. Once received, two photocopies of all file material are made. One copy is edited and forwarded to Crown Council for the case at Justice. The second copy remains unedited and is also forwarded to Justice. Relevant information from the file is forwarded by Child and Family Services' Crown Council to the plaintiff's lawyer with the Statement as to Documents. The original file is kept in Central Office until the case is concluded. Copies of the claim (which essentially is the request) and all other material pertaining to the claim are kept in central filing.

17. Social Services (continued)

4. Freedom of Information requests

These requests are sent to a central staff person who records the request, creates a file folder and distributes the requests to representatives in each Division. From there, the Divisional representative handles the request. For Child and Family Services Division, the procedures are as follows. The FOI form is forwarded to Manager, Litigation Support. An ACI (Automated Client Index, i.e., client profile created by Social Services) inquiry into Child and Family Services' involvement with the requester is completed.

From this inquiry it becomes apparent what regional office the client's involvement originated. The Program Manager from that regional office is contacted and the approach to contacting the requester and sharing the information is discussed. A letter is sent to the requester (within 30 days of receiving the FOI request) providing the name and number of the Program Manager who they can be in touch with who will share their information with them. The Program Manager is copied on the letter.

At times, the file material is summarized by the regional office into a brief document, which the Program Manager presents to the individual. This is especially true if the file is very large and would be quite time consuming to review. Other times, the Program Manager will sit down with the requester while the file is reviewed. All references to third parties must be removed prior to sharing the file. File material is not handed over to the requester. Centrally, a copy of the letter to the requester is kept with the central file and it is stored.

When Child and Family Services provide information to lawyers, the information is shared with the following stipulated trust conditions: that the documentation not be copied or reproduced in any manner; that the documentation remain on the client file at all times; that the documentation only be used for the preparation of the client and case in the present litigation and for no other purpose; that the documentation not be disclosed to any person other than the client or clients represented by the lawyer and their firm in the legal proceedings or other than to relevant witnesses who are under oath in the legal proceedings, unless Justice has provided the lawyer with written consent to do so; and, that if the lawyer's client requests the file from the lawyer by way of termination of solicitor/client relationships or if the file is authorized by the lawyer's client to be transferred to another law firm, that the documentation be returned to Justice.

In all cases if Child and Family Services has questions or issues regarding the disclosure of personal information, Justice is consulted.

17. Social Services (continued)

The Income Security Division routinely releases the paper and electronic file information about benefits and the chronological recordings to individuals. Excluded from the releases are any third party comments and the Family Services program assessments. The Division requires that two staff handle each inquiry. If the authority to release the information is unclear, the Division consults with a solicitor where required.

Social Services will delete, update or add to, an individual's personal information where it is shown to be inaccurate, incomplete or out-of-date. Client records are continually maintained through processes such as client reporting, system interface updates, and through the audit/verification process. The majority of the changes are client initiated or through direct data sources. Where information, other than the client reported, results in a change to the client's eligibility for a certain program, they are informed by letter.

The Community Living Division will update an individual's personal information where it is shown to be inaccurate and has been confirmed with the client, family or service provider.

CHALLENGING COMPLIANCE

Housing Services does not have a formal process in place to deal with complaints about its personal information management practices.

Each of the Divisions of Social Services, other than Housing Service, have a formal process in place to deal with complaints about their personal information management practices or policies. The formal process to handle complaints is to make an application through *FOI*. Alternatively, complaints are directed to a supervisor or manager who in turn will assess and escalate if necessary. At the Valley View Centre complaints are reviewed by the Human Resources Department and the Director of the Centre before being escalated if necessary.

Child and Family Services has received complaints in the past 12 months regarding its personal information management practices. Minister's Referrals have been received indicating that workers have not maintained confidentiality. All complaints are thoroughly reviewed. The complaints generally relate to child protection cases where individuals that make a child protection report/referral are advised that their name will be kept confidential unless they are required to attend court. However, in some situations the client is able to determine who made the referral and it may appear that there was a breach of confidentiality, when in fact there may not have been.

17. Social Services (continued)

The Income Security Division has received a complaint regarding its personal information management practices over the last 12 months. The complaint went through the Privacy Commissioner and it is the Division's understanding that it was unfounded.

The Housing Services Division had an incident in the past 24 months relating to the Repair Programs where an individual's tax returns were mistakenly sent to a wrong address. A letter of apology was issued to the individual and the incident was discussed with the staff involved to ensure that such an incident would not occur again.

Currently two staff are being investigated for the potential breach of policies and procedures pertaining to the handling of personal information. Whether or not policies and procedures were breached is to be determined.

RECOMMENDATIONS

1. Social Services should continue to provide regular training for all employees with respect to the handling of personal information and should consider implementing ongoing, mandatory training and formal re-enforcement of *The FOI Act* and privacy principles.
2. Social Services should develop policies and procedures that support the overall privacy framework of the Government of Saskatchewan. Employees should review privacy policies annually and should signify this review with an annual sign-off that they understand the principles of privacy.
3. Social Services should establish overall accountability for privacy within the Department.
4. In the development of contracts with outside parties, the Department should ensure that protection of personal information clauses are built into contracts. This should be consistent with the direction of the Government as a whole. Where the Department provides information about an identifiable individual to a third party, such as for processing, the third party should be contractually bound to abide by the Department's personal information (privacy) requirements.
5. Social Services should ensure that regular reviews are implemented to ensure compliance with *FOI* principles and the privacy framework. This should include regular reviews of the safeguards in place to protect personal information (such as technology audits).

17. Social Services (continued)

6. Social Services should continue to work towards implementing a formal system for the identification of the type of personal information it collects and the classification of the information as to sensitivity to determine the appropriate levels of safeguard for such information. The Department should use the government's data classification scheme (to be developed) to assist them in this process.
7. Social Services should review all policies and procedures with respect to the information collected, retained, handled and destroyed by the Department. These policies and procedures need to balance the requirements identified in the policies with privacy considerations.
8. Social Services should continue to address the recommendations made by the Provincial Auditor in their 1999 report on IT security.



Appendix B