Culture of Care…or Culture of Surveillance?

Personal Privacy and the BC Government's Integrated Case Management System: Legal, ethical and procedural implications for independent community service organizations

BC Freedom of Information and Privacy Association
in association with the
United Community Services Co-operative of BC
with the financial support of
The Law Foundation of British Columbia

March 2010

www.privacyresearch.ca

FIPA and the UCS Co-op wish to acknowledge
the Law Foundation of British Columbia
for funding this project and for their ongoing support of
law reform, legal research and public legal education
in British Columbia

www.lawfoundationbc.org

BC Freedom of Information and Privacy Association

103 - 1093 West Broadway
Vancouver, BC V6H 1E2
Ph: 604-739-9788
Fax: 604-739-9148
Email: fipa (at) vcn.bc.ca
Web:www.fipa.bc.ca

United Community Services Co-operative of BC

201-1638 East Broadway
Vancouver, BC V5N 1W1
Ph: 604-687-2919
Fax: 604-488-1022
Email: info (at) ucscoop.com
Website: www.ucscoop.com

Table of Contents

Acknowledgements

Culture of Care or Culture of Surveillance? would not have been possible without the expertise and efforts of the following:

Research Team
- Martha Rans, Barrister and Solicitor (Lead Researcher)
- Cassandra Florio (Assistant Researcher)
- Vandana Sood (Assistant Researcher)
- Alison Marshall, Consultant, United Community Services Co-op

Writing Team
- Tim Beachy, Chief Executive Officer, United Community Services Co-op
- Darrell Evans, Executive Director, BC Freedom of Information and Privacy Association
- Gerald Fahey, Barrister and Solicitor, MacDonald Fahey Barristers & Solicitors
- Vincent Gogolek, Policy Director, BC Freedom of Information and Privacy Association
- Justin Ho, Manager, United Community Services Co-op
- Martha Rans, Barrister and Solicitor

Project Steering Committee
- Tim Agg, Executive Director, PLEA Community Services
- Tim Beachy, Chief Executive Officer, United Community Services Co-op
- Darrell Evans, Executive Director, BC Freedom of Information and Privacy Association
- Vincent Gogolek, Policy Director, BC Freedom of Information and Privacy Association
- Ross Harvey, Executive Director, BC Persons with AIDS Society
- Justin Ho, Manager, United Community Services Co-op

Project Advisors
- Gerald Fahey, Barrister and Solicitor, MacDonald Fahey Barristers & Solicitors
- Micheal Vonn, Policy Director, BC Civil Liberties Association

Participating Case Study Organizations
- Abbotsford Community Services – Abbotsford
- Fraserside Community Services Society – New Westminster
- PLEA Community Services Society – Vancouver
- Victoria Transition House Society – Victoria

Introduction

Every day, hundreds of thousands of British Columbians walk through the doors of community organizations across BC looking for help. They are people with families in crisis, individuals looking for counseling support, employment transition help or health services – to name a few. Many of these individuals provide all sorts of personal information as part of obtaining help from either community-driven services or provincial government programs. They have little knowledge of how their personal information is stored, managed, or shared, but they have a right to know that their information is handled in the most ethical and legal manner, and to withhold their personal information should they choose to do so.

– Privacy Project Steering Committee

Project Description

This study, known colloquially by its participants as "The Privacy Project", was initiated by the BC Freedom of Information and Privacy Association and the United Community Services Co-operative based on our shared interest in five issues that are of growing concern among the independent community service sector in BC. Specifically, concern is mounting among independent community service organizations (hereafter referred to as "ICSOs") about:

- the organizations' ongoing ability to protect the privacy of their clients in the face of increasing demands for access to their clients' personal information by all levels of government, but particularly by the government of British Columbia;
- their ability to ensure that clients have an appropriate level of consent and control over what information about them is shared with other persons and institutions;
- the potential loss of organizational ability to build trusting and enduring relationships with clients, due to clients' perceptions of threats to their privacy;
- the onerous responsibilities, skills and accountability required of ICSOs and their often ill-equipped privacy officers, in light of rapidly-changing information technology and the volume and complexity of services for which they are contracted and funded by external, mostly provincial government, sources; and,
- the legal risks and liabilities accruing to directors and officers of these charitable and non-profit organizations in consequence of new technologies, new contractual relationships, and new laws and regulations surrounding the services they deliver in the community.

These issues have taken on new urgency with the recent decision[1] by the BC Government to develop an "Integrated Case Management and Contract and Supplier Management system." This system has the ambitious objective of gathering, and sharing across government, personal information obtained from people receiving virtually all government services – not only the services delivered by government proper, but services delivered by arm's-length community service organizations as well.

Major Themes of the Study

The Key Issue

As part of a global trend towards consolidating the management of government-held information, there is an initiative underway within three British Columbia government ministries to create an integrated case management system. This new system will collect, store and disclose the personal information of the clients of these Ministries' programs, whether the clients are served directly or through out-sourced services operated by contracted third party organizations or ICSOs.

The key issue of concern to organizations in the sector, and the problem which we attempt to address in this study, was defined as follows:

> The Province, through several different Ministries, contracts out over $1.8B in social, employment and health services each year, covering a wide range of service and organizational types. The planned integrated case management system represents a major change in the legal environment and procedures and protocols for the thousands of community and non-profit organizations across BC contracted to provide services on behalf of the Government of BC.
>
> ICSOs are ill-equipped to fully analyze, understand and be accountable for the legal, ethical and procedural issues involved in owning, holding custody of, disclosing to third parties, and protecting the privacy of client information of such profound sensitivity within the proposed integrated case management system (ICM).
>
> The implementation of this new system will have many implications, including extremely complex systemic changes in the way detailed personal information about clients is managed, protected, and transferred to and from these Ministries by community organizations.

Because Integrated Case Management (ICM) represents a profound change in the way personal information is managed, affecting hundreds of ICSOs and hundreds of thousands of people in British Columbia, FIPA and the UCS Co-op agreed to ask the Law Foundation of British Columbia to consider funding a study into the proposed system under the Foundation's Large Projects Initiative. The Foundation agreed to fund the project in 2008.

[1] Speech From the Throne, February 9, 2010. MHSD press release February 12, 2010 http://www2.news.gov.bc.ca/news_releases_2009-2013/2010HSD0021-000152.htm

The Purpose of the Study

The purpose of the study was as follows:

> To fully understand the privacy impact and the legal, ethical and procedural implications of the integrated case management system proposed by three Ministries of the Provincial Government.

The rights of individuals served through these independent community service organizations to privacy and informed consent regarding the collection, use and disclosure of their personal information are at the centre of this initiative. Those individual rights provide the moral anchor to the work of the project, as ultimately the risk to community organizations is directly related to their ability or inability to protect the privacy rights of their clients.

Stakeholder Engagement

The study was accomplished with direct participation by representatives of community-based charitable and non-profit service organizations. A wide range of these groups were invited to help steer and advise the project and to participate in an on-line survey regarding the role and work of individual Privacy Officers.

Members of the project advisory board and project team also met on several occasions for briefings and dialogue with representatives of the British Columbia government, including the province's Chief Information Officer and officials from the Ministry of Children and Family Development, Ministry of Health Services, and Ministry of Citizens' Services.

Hoped-for Outcomes

The conclusions and recommendations of this study should be seen as a direct and serious challenge to the assumptions at the foundation of the ICM project, which we conclude present major risks for government, for ICSOs, for client relationships, and for the privacy rights of individuals. Sober second thought about the project is more than warranted.

In our communications with BC government officials during this project, we proposed that this study be accepted as our contribution to a formal government consultation on all aspects of the proposed ICM system and its implementation. The officials expressed some willingness to consider creating such a consultation process. We hope they will do so in the near future.

Executive Summary of Findings and Recommendations

Protecting privacy in the digital age: "Only the right information, to only the right people at only the right time."

We live in a digital age. Much of what was once done by hand, with pen and paper, is now being done with electronic devices and records. These electronic marvels can be hugely beneficial in terms of delivering services more effectively and efficiently while reducing costs – but they also bring their own set of risks.

When it comes to the delivery of social services to vulnerable people by Independent Community Service Organizations (ICSOs), the biggest risks of the digital age are:

- the transformation of ICSOs into collectors of personal information for, and agents of, the State,
- a potential decline of service quality due to the loss of the relationship of confidentiality and trust ICSOs need to serve people effectively, and
- excessive and inappropriate scrutiny by government into the private lives of citizens receiving social services.

The findings of this study should sound a clear warning to government, the independent community service sector, and the general public that all is not well with the BC government's plan for what is called "Integrated Case Management" (ICM).

The planned ICM system would be an unprecedented grab by the government for the personal information of the clients of independent community service agencies, and unprecedented license to merge, use and disclose that information to a wide range of parties without the consent of either the clients or the agencies.

As described in the government's own materials quoted in this study, the ICM System would provide government officials with access to extensive information about BC citizens' daily lives. The system would enable information sharing between the Ministry of Child and Family Development (MCFD), and other ministries. The information grab would not stop within government proper – it would extend well beyond to capture the independent agencies contracted by government to provide services to the community.

The ramifications for such an unprecedented proliferation of data disclosures between the government and the private sector are vast and deeply troubling. If privacy is the underlying value of our freedom and liberty, as Ann Cavoukian[2] says, we need to carefully consider the risks posed by the imposition of a data information sharing system that does not appear to recognize the boundaries between what is private and what is public.

This report also concludes that ICM could seriously degrade services to the public by radically changing the culture of the independent community service sector.

The organizations that make up this sector are mostly non-profits and charities created by small groups of individuals with a specific mission, an extraordinary level of commitment to serve the community, and an entrepreneurial approach. The difficulty inherent in starting and sustaining such groups can hardly be overestimated. This level of human creativity and drive can rarely be sourced within governments, which is why governments seek partnerships with ICSOs.

If ICSOs do their job of service well, they may grow rapidly and be recognized by various government and private sector bodies as effective, efficient and low-cost ways of delivering services to a needy part of the community.

The proposed ICM system has the potential to transform this culture from one where helping people in distress is paramount to one where service organizations are *de facto* agents of the state, with the function of funneling their clients' most intimate personal information to the provincial bureaucracy. Many of the virtues which cause governments to seek to deliver services through ICSOs in the first place could be lost, at great cost to society.

Major Findings

The results of this study and its engagement with organizations that will be affected by the ICM system indicate the need for an immediate and massive system-wide effort to clean up the cluttered and complex legal and procedural environment, clear out the confusion, and ensure a safe information environment for clients, workers, service organizations and government.

It is not prudent, safe, or responsible to introduce a single sector-wide ICM system into an environment where there is a desperate need to update and modernize information management and privacy protection technology and practices.

Ministries of the provincial government are currently working with outdated contracts and systems that desperately need replacement. Most non-profit organizations have few or no electronic systems, and no resources to acquire this infrastructure.

Spending millions of dollars of taxpayers' money to build an ICM system before all stakeholders, in common cause, resolve the issues identified in this paper would be putting the cart before the horse, with potentially disastrous outcomes for all parties involved.

[2] Ann Cavoukian is the Information and Privacy Commissioner of Ontario

The major findings of this initial research are, quite simply, astonishing. This is an extremely complex informational environment with:

- overlapping legal frameworks;
- little jurisprudence or analytical work to frame the issues;
- very high pressure to "give funders everything they want";
- contractual relationships that differ widely between and among ministries of the provincial government, federal departments, and other funding sources;
- little documentation of best practices or training towards quality control, and
- little or no awareness on the part of clients as to their information rights and how (or why) to exercise them.

As a result, confusion reigns both on the ground and at the highest levels – from the front-line worker and the clients with whom they have confidential relationships, to the Privacy Commissioner and onward to the Legislature.

Complicated contractual and reporting requirements overlap, sometimes appearing to circumvent the *Freedom of Information and Protection of Privacy Act* requirements for public bodies and the *Personal Information and Privacy Act* requirements for private and non-profit organizations.

The proposed ICM system will add yet another layer of requirements and technical complexity. Rather than serving to clarify the situation, it will add to the confusion.

Protecting privacy in the Independent Community Service Sector

The ICM system has the potential to transform the existing relationship between service providers and government, essentially removing the borders that currently exist between them. All aspects of a client's life may flow through the system to various bureaucrats in various government departments.

Protecting the confidentiality of client information is a fundamental principle of the ICSO sector:

> Privacy of personal information goes to the heart of our identity as human beings and is fundamental to a person's dignity, integrity and autonomy. Privacy is necessary for health. An individual's sense of identity, dignity, self-esteem, competence and personal choice are recognized as critical elements within the principles of psychosocial rehabilitation and recovery.
>
> However, self-disclosure is also linked to mental health, and the expectation of confidentiality in the therapeutic relationship can open the way for willing disclosure of sensitive personal health information. . . . *Providers believe that if clients do not trust that their personal health information will be protected, they will be reluctant to fully and honestly share personal health details and may avoid seeking care altogether*[3].

[3] Goldner, Elliot M., Judith Tompkins, and Karen Cardiff, "Mental Health On-line: A Case for Information Management", final report made to Health Transition Fund, Health Canada February 2001, [Mental Health On-line] at pp. 25-26.

Legal Issues

The legal research undertaken for this project was framed by three factors that must be considered in current institutional environments in order to correctly manage personal information: statutory privacy rights, including a reasonable degree of control by individuals of their own personal information; confidentiality and consent in relationships of trust; and security of personal information.

The legal issues at stake are fundamental, and go to the heart of a civil society. They include:

- the privacy rights of citizens;
- the individual's right to confidentiality in therapeutic relationships;
- the individual's right to control dissemination of personal information;
- the need to control institutional information and protect the rights of directors and officers of those institutions;
- the need to have contractual relationships that are legal in all aspects, and
- the need for adequate resources to properly manage and secure personal information.

The Right to Privacy in Canada

The right to privacy is something all Canadians expect, and it is guaranteed under the *Charter of Rights and Freedoms*.[4]

The Supreme Court of Canada has ruled that the Constitution protects "a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[5] [Emphasis added.]

Our privacy rights are also protected under privacy legislation when our information is provided to provincial government bodies (which are covered by the *Freedom of Information and Protection of Privacy Act* or FIPPA) or non-governmental or private sector organizations (which are covered by the *Personal Information Protection Act* or PIPA). These Acts set out the framework for how personal information is to be collected, and in what circumstances it can be shared, used and disclosed.

One of the main objectives of privacy legislation is to protect personal privacy by "preventing the unauthorized collection, use or disclosure of personal information by public bodies."

---

[4] Section 7 deals with "life liberty and security of the person and the right not to be deprived therof except in accordance with the principles of fundamental justice. Section 8 protects against "unreasonable search and seizure", and s. 12 states that "everyone has the right not be subjected to any cruel and unusual treatment or punishment.

[5] *R.* v. *Plant*,[1993] S.C.J. No. 97 (Q.L.), para. 19.

Privacy and Control

The goal of privacy legislation is to ensure that the core of an individual's personal information is theirs to preserve and dispose of as they see fit. It does so by establishing that each individual has a defined set of rights regarding the collection, use and disclosure of their personal information by organizations and other individuals.

Our research suggests that, in light of changing contract language, there is increasing confusion around who actually owns the personal information once a client divulges it to an ICSO. The proposed ICM system poses a tremendous risk as it could remove existing privacy safeguards once the information is collected in an electronic form.

Confidentiality and Consent

Confidentiality and the individual's right to consent to the collection, use and disclosure of their personal information, though not absolute, are key elements in establishing trust in relationships between service providers and their clients.

For street-entrenched youth, women fleeing violence, people with special needs and a multitude of others using social services, the relationship between themselves and their service provider is built on and dependent upon trust. For all community service organizations, the protection of client privacy is key to their ability to engender and sustain that trust: information is not disclosed outside the circle of care without a pressing, substantial and legally sanctioned reason.

The ICM system poses real challenges to the sector's ability to ensure the confidentiality of their clients' information in the face of broad government powers to collect, collate and distribute that information.

Security

Breaches of database security are endemic, both within government and the private sector. Privacy legislation and institutional practices have not kept pace with technological changes that have facilitated a rising tide of security breaches and computer-based crime. Significant additional resources will be required to ensure even minimal safeguards can be implemented by the independent community service sector.

Once personal information is improperly or illegally disclosed, irreparable damage may be done to individuals and organizations. In light of these factors, the increased risk of inappropriate disclosure through the proposed ICM system is unacceptable.

Conclusions

We conclude that an ICM system that has the capability to harvest, store, inter-relate and disclose vast amounts of data about individuals, families, groups and communities constitutes an unprecedented invasion of the privacy of citizens, will inevitably over-

reach, engendering public resistance, and eventually could destroy both the legal and moral credibility of ICSOs and their ability to function effectively.

The creation by the State of this type of 'Big Brother' data system has sparked wide public outrage before in Canada. A project of this nature is shortsighted and would ultimately be counter-productive to the very results the government wishes to achieve by instituting the system.

BC's Chief Information Officer defined the overall objective of the ICM system as: "The right information to the right people at the right time". One of the community representatives engaged in this initiative provided the necessary qualification: "Yes, but it should be **only** the right information, to **only** the right people, at **only** the right time." There may be only one word of difference between the two paradigms, but that word makes a world of difference.

Overview of Recommendations

Our recommendations fall into three groups: Those made to clients, those made to colleagues in the community sector and those made to government.

It is understood that, in some few cases, pressing circumstances may arise that require exceptions to the privacy-sensitive regime of information management proposed in these recommendations. But for such cases, all parties should exercise extreme caution and any proposed deviation should be authorized by statute, strictly limited, and subject to the oversight and approval of the province's Information and Privacy Commissioner.

- Clients are entitled to responsive information management systems that meet the highest ethical and legal standards. They must be informed of their privacy rights in a manner which ensures they understand these rights and which empowers them to make informed choices.

- People working in the independent community service sector must have clarity in understanding and carrying out their obligations to both clients and contracting sources. They must be included in a new dialogue to design a better framework for information management and privacy protection.

- Government must understand the need for a negotiated and shared framework and approach to personal information management systems. They must recognize the arms-length nature of ICSOs and this recognition must be reflected in contractual relationships.

The full list of recommendations proceeding from this study may be found in the "Conclusions and Recommendations" section – see page 43.

Understanding the Issues and Getting the Context

Protecting Privacy in the Digital Age: "Only the right information, to only the right people at only the right time."

> *It's not that privacy is dead…it's that it's changing... It's being transformed in this new online world of ubiquitous data availability. The reason privacy is not dead and will never die is because privacy forms the basis of all of our freedoms and our liberty.*[6]

We live in a digital age. Much of what was once done by hand, with pen and paper, is now being done with electronic devices and records. These electronic marvels can be hugely beneficial in terms of delivering services more effectively and efficiently while significantly reducing costs – but they also bring their own set of risks, particularly in the areas of service quality and privacy.

This report presents the results of an independent investigation into a new government initiative that is bringing the digital age to the health and social services sectors in the province of British Columbia. The initiative is called the "Social Sector Integrated Case Management Project", and it is defined in the following terms in government documents:

> In 2005, the Province set out "Five Great Goals for a Golden Decade" to help British Columbia realize its full potential as the best place on earth to raise a family, to live and play, and to work, invest, and get ahead. Great Goal 3 commits to building the best system of support in Canada for persons with disabilities, those with special needs, children at risk and seniors. To achieve this goal, service delivery will need to be collaborative and citizen-centred – not from one organization alone, but across the social sector.
>
> The Office of the Chief Information Officer in the Ministry of Labour and Citizens' Services is leading the Social Sector Integrated Information Management Project to develop a secure, privacy-protected information sharing framework and a context for Integrated Case Management and Contract and Supplier Management. This will provide the holistic view of each citizen required to truly

[6] Ann Cavoukian, Information and Privacy Commissioner for Ontario, The Globe and Mail, Sept. 13, 2008.

integrate delivery of social services in support of Great Goal 3, linking case information collected by other organizations delivering services to the public, such as the ministries of Health, Education, and the Attorney General, other provinces, the federal government, and Service Delivery Providers.[7]

This investigation was initiated because a group of independent community social service providers became alarmed at the extraordinary new demands that would be made by government for access to the personal information of clients under the Integrated Case Management (ICM) System. These organizations were concerned about the ethical, legal and procedural ramifications of ICM for their organizations and for relationships with their clients.

This report concludes that, while it may have some very worthy goals, the government's vision would be more characteristic of a "Surveillance Society" than a New Golden Decade of service to the public.

The Integrated Case Management System as envisioned would provide government officials with unprecedented access to extensive information about BC citizens' daily lives. The system would enable information sharing between the Ministry of Child and Family Development (MCFD), and other ministries. The holistic information collection would not stop within government – it will extend well beyond to capture the independent community service organizations contracted by government to provide services to the community.

The ramifications for such an unprecedented proliferation of data disclosures between the government and the private sector are vast and deeply troubling. If privacy is the underlying value of our freedom and liberty as Ann Cavoukian says, we need to carefully consider the risks posed by the imposition of a data information sharing system that does not appear to recognize the boundaries between what is private and what is public.

This report also concludes that ICM could seriously degrade services to the public by radically changing the culture of the independent community service sector.

These groups – mostly non-profits and charities – are usually created by a small group of individuals with a mission, commitment and an entrepreneurial approach. The difficulty inherent in starting and sustaining such groups can hardly be overestimated. If they do their job of service well, they grow and may eventually be recognized by the state as an effective, efficient and low-cost way of delivering services to a needy part of the community.

ICM has the potential to transform that culture from one where helping people in distress is paramount to one where organizations are de facto agents of the state, with the function of funneling their clients' most intimate personal information to the provincial bureaucracy.

[7] Ministry of Employment and Income Assistance, "Request for Proposals: Case Management Software [RFP] SATP-239", November 6, 2007at p. 9. Reiterated in **SATP-270, February 5, 2009 para 4.2**

The Proposed Integrated Case Management (ICM) System: What it means for information sharing

The ICM system is the foundation of a proposed overarching plan called the Social Sector Integrated Information Management project. Its vision is:

> The right information, to the right people, at the right time, in a secure manner that protects privacy to improve outcomes for citizens through the cohesive delivery of social services. This includes timely access to personal information for front-line staff to facilitate provision of services to citizens, as well as anonymous aggregate information for research, evaluation and planning at the program, ministry and sector level.[8]

In the BC government's Five Great Goals for a Golden Decade, Great Goal 3 commits to building a system of support for persons with disabilities, special needs, children at risk and seniors[9]. The ICM proposes to do so by "taking a holistic view of each citizen", and integrating social service delivery by "information sharing across the social sector"[10].

> The sharing of information between ministry staff and Service Delivery Providers is a critical part of achieving a comprehensive view of the client, managing ongoing services, and informing decision-making at all levels of both organization [sic.]. As a result, replacing technology alone will not be sufficient to meet business and strategic goals and as such, the ministries have analyzed the optimal approach with their Service Delivery Providers.[11]

There may well be potential for improvement with the development of better systems and provision of increased resources, training and education, but the government has not made the case for this unprecedented demand for the disclosure of detailed client data from non-governmental service providers and why it is necessary for effective programming. Nor, in our opinion, has the government fully recognized the risks inherent in such disclosure.

The ICM system represents a radical departure from the way community service organizations relate to and serve their clients. It poses real challenges to the sector's ability to ensure the confidentiality and security of their clients' information in the face of broad state powers to collect and use personal information. Specifically:

- The ICM vision disregards clients' expectations of privacy and the responsibility of community service organizations to protect client privacy;
- ICM documents contain few references to privacy protection, fewer still to client expectations of privacy, and none to the need for client consent for the disclosure and usage of their personal information; and

---

[8] *Ibid.* See also **SATP-270, February 5, 2009 p.50-1**

[9] *Ibid.*

[10] *Ibid.* at p.10. See also **SATP-270, February 5, 2009 p.11**

[11] *Ibid.* at pp. 23-24. See also **SATP-270, February 5, 2009 p.50-1**

- The ICM system does not have clearly articulated methods to ensure the safeguarding of clients' sensitive personal information.

For street - entrenched youth, women fleeing violence, people with special needs and a multitude of others who access social services, the relationship with their service provider is built and dependent upon a relationship of trust. For community social service providers, the ability to engender that trust depends greatly on their respect for their clients' privacy and their ability to protect it.

The prejudice to individuals from privacy violations is real. Violations of privacy strike at the heart of who we are. There has been little in government descriptions of the ICM system or our subsequent discussions with government officials to give the community social service sector comfort that our clients' privacy rights will be respected or safeguarded in the new system.

There may already be serious flaws in the information-sharing framework upon which ICM would be based. There is an urgent need to stop and evaluate the extent to which the new system can assure respect for the core value of privacy. For a sector that spends over a billion dollars a year caring for the sick, vulnerable and marginalized members of our community, we need to ask whether ICM will ensure that *only* the right information, gets to *only* the right people, at *only* the right time.

Privacy and its Importance in Canadian Society

The Supreme Court of Canada has repeatedly affirmed that laws embodying the right to privacy enjoy a quasi-constitutional status[12].

The right to privacy is essential to all Canadians, and it is guaranteed under sections 7, 8 and s.12 of the *Charter of Rights and Freedoms*.[13] The Supreme Court of Canada has made strong statements about the importance of the right to privacy in a number of different contexts. Madam Justice L'Heureux - Dube in *R. v. O'Connor* stated:

> Respect for individual privacy is an essential component of what it means to be free. . . When a private document or record is revealed the invasion is not with respect to the particular document or record in question. Rather, it is an invasion of the dignity and self-worth of the individual, *who enjoys the right to privacy as an essential aspect of his or her liberty* in a free and democratic society[14]. [Emphasis added]

The right to privacy with respect to documents and records was addressed by the Supreme Court in *R.* v. *Plant* as follows:

---

[12] See *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 and *R. v. Duarte,* [1990] 1 S.C.R. 30 (S.C.C.)

[13] Section 7 deals with "life liberty and security of the person and the right not to be deprived therof except in accordance with the principles of fundamental justice. Section 8 protects against "unreasonable search and seizure", and s. 12 states that "everyone has the right not be subjected to any cruel and unusual treatment or punishment.

[14] *R. v. O'Connor* [1995] 4 S.C.R. 411 at paras. 114, 119.

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* seek to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[15] [Emphasis added.]

The courts have set out a number of different types of privacy rights in different situations, but personal medical information has been accorded the highest degree of protection. With respect to health information, the SCC has recognized that individuals maintain an ongoing privacy interest in their health information after it has been collected and is in the hands of health care providers. In *McInerney v. MacDonald*, Justice LaForest observed:

> [M]edical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient.[16]

At the provincial level in BC, privacy rights are protected by the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") which covers the public sector and the *Personal Information Protection Act* ("*PIPA*") which covers the private and non-profit sectors.[17].

Both of these Acts set out the framework for how personal information is to be collected, and in what circumstances it can be shared, used and disclosed. One of the main objectives of privacy legislation, including *FIPPA*, *PIPA* and the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[18], is to protect personal privacy by "preventing the unauthorized collection, use or disclosure of personal information by public bodies."[19]

Personal Information Protection Act ("PIPA") Requirements

In meeting its responsibilities under *PIPA*, a private sector or non-profit organization must consider "what a reasonable person would consider appropriate in the circumstances."[20]

These private and non-profit organizations must also "develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act."[21]

---

[15] *R.* v. *Plant*,[1993] S.C.J. No. 97 (Q.L.), para. 19 [hereinafter *Plant*].
[16] *McInerney v. MacDonald* [1992] 2 S.C.R. 138 at para. 18.
[17] R.S.B.C. 1996, c.165 [*FIPPA*] and S.B.C. 2003, c. 63 [*PIPA*], respectively.
[18] *Personal Information Protection and Electronic Documents Act,* R.S. 2000, c.5. [*PIPEDA*]
[19] *FIPPA*, op cit note 17, s.2(d).
[20] PIPA s.4(1)
[21] ibid. s.5 (a)

Further, under *PIPA*:

> An organization must not collect, use or disclose personal information about an individual, without either the consent of the individual, under statutory authority or where PIPA deems that consent has been given.[22]
>
> Before collecting personal information about an individual from the individual, an organization must disclose the purposes for the collection of the information to the individual verbally or in writing, as well as contact information for someone who can answer questions about the collection.[23]
>
> Before collecting personal information about an individual from another organization without the consent of the individual, an organization must provide the other organization with sufficient information regarding the purpose of the collection to allow that other organization to determine whether the disclosure would be in accordance with this Act.[24]

Social & Health Services in Our Community: Who we are and what matters to us

Independent Community Service Organizations (ICSOs), which make up what is generally known as the community social service sector, play a crucial role in meeting the varied and vital needs of many people in the province of British Columbia, including the most vulnerable and marginalized members of our community.

- According to Statistics Canada, in 2003 about 1,800 of BC's 20,000 non-profits were in the social service sector;
- Many ministries have the majority of their services delivered by non-profits, in some cases as much as 99 percent[25]; and,
- Independent Community Service Organizations employ thousands of people, with many more volunteer workers also delivering services.

Few of us can say we have never walked through the doors of a community service agency.

As part of this research project, we undertook a survey of 36 ICSOs that provide services that would make them subject to the proposed Integrated Case Management system [26]. More detail about the survey and other extensive research with ICSOs is provided in the

---

[22] ibid., s.6. but note also the specific situations set out in s. 12 where consent is not required.
[23] Ibid., s.10(1)
[24] Ibid., s.10(2)
[25] *A Report on the Interface between the Social Development Ministries and the Non-Profit Sector* Cross Government Research, Policy And Practice Branch, Office Of The Chief Information Officer, Ministry Of Labour And Citizens' Services, 2008 p.4 .
[26] These organizations compose a subset of the membership of the United Community Services Co-op.

following section on Research. In brief, a number of common characteristics were apparent from the responses of these organizations, including:

- The diversity and sometimes contradictory responses to our questions clearly describe a complex privacy landscape in which organizations operate;
- 91% of organizations reported that they received some form of provincial government funding;
- Of the organizations with multiple-source funded programs, 66% said that managing projects with conflicting reporting requirements was somewhat or very difficult; and,
- Over 40% reported that available resources for managing privacy were inadequate in terms of finance, training and/or allocation of staff time.

For many people walking through the doors of an independent community service organization, the social services they receive are their lifeline. The privacy issues identified through this research project are many and their impacts on how organizations are able to serve their clients, build a trusting relationship, and provide the vital support needed is profound.

The Research

When planning this important research initiative, we were clearly aware of the complexity of the social service sector and the independent community service organizations that provide vital services and programs to British Columbians across the Province.

Doing any meaningful legal research would mean framing it within this complexity. This frame of reference was developed by two additional research activities that supported the legal research undertaken:

1. A comprehensive survey of a representative group of ICSOs to gauge their overall impressions of the privacy landscape in relation to how they serve their clients; and,
2. More comprehensive site visits with four select ICSOs to review (with a lens on privacy and the proposed ICM) how they deliver services to clients and how they manage and administer client information.

Getting a Scan: Surveying Independent Community Service Organizations

As a partner in this research, the United Community Services Co-op surveyed its membership of 110 organizations. All but a handful of members are independent community service organizations, representing the diversity of the various facets of the social service sector from all across the Province.

Thirty-six responses were received and a number of common themes emerged from the answers given by organizations, including:

1. Organizations are ***operating in a complex environment*** and one that is strongly ***reliant on government funds***:
    a. On average, ICSOs were operating 20 programs and services each, 720 separate programs and services in total;
    b. 91% of organizations reported that they received some form of provincial government funding;
    c. Over 40% of organizations had all of the programs funded by government;
    d. Of the organizations with multiple-source funded programs, 66% said that managing projects with conflicting reporting requirements was somewhat or very difficult; and,

e. No consistency exists on the practice of how client notes are documented – from paper (81%) to paper only after the visit (44%) to paper and then re-entered electronically (44%) to electronic recording while with the client (28%) to other (16%) to some combination of the above.

2. ***Confusion exists on the key issues related to privacy*** amongst organizations:
    a. When asked about ownership of client information, 10% noted that clients themselves owned their information, 55% said organizations do, while 35% said government did.
    b. The diversity of responses to the qualitative questions of the survey also reflect a level of confusion and conflicting viewpoints on key privacy issues. See Appendix B for detailed responses.

3. ***Privacy is paramount in the therapeutic relationship*** between organizations and their clients – 100% noted that confidentiality with their clients is "very important".

4. ***More resources are needed*** to ensure proper privacy protocols and procedures are in place at ICSOs:
    a. Over 40% reported that available resources for managing privacy were inadequate in terms of finance, training and/or allocation of staff time.
    b. Only 18% reported being able to very adequately train staff on privacy issues and protocols.

Complete results from the survey, as well as a complete list of questions, are available in Appendices A and B.

Going Deeper: More in-depth with four organizations

The survey of ICSOs provided some overarching context around client and privacy realities for the sector, but in many cases the implications of a proposed ICM can best be analyzed when specifically juxtaposed to the actual operations of impacted organizations.

Process

To get down to that level of detail, the need to conduct site visits with a handful of organizations was identified and four organizations accepted our request for an in-depth site visit. They were:

1. Abbotsford Community Services Society
2. Fraserside Community Services Society
3. PLEA Community Services Society of BC
4. Victoria Women's Transition

In depth engagement with each organization involved one extensive site-visit with key staff, as well as follow-up conversations and correspondences as required. Confidentiality forms were signed with each organization, ensuring the information gathered would be aggregated in order to observe trends.

We reviewed with each organization myriad pieces of information, which included the following:

- Service and contribution relationships with funders;
- Client contact procedures and forms;
- Privacy and information management procedures and infrastructure; and,
- A sampling of case files.

Conclusions

From these visits, a few broad observations can be made:

1. The amount of sensitive personal information collected on each client is considerable; and,
2. The consequences of the disclosure of personal information to the government are potentially enormous. Our research has indicated that clients may choose not to avail themselves of necessary services if their personal information is not confidential within the ICSO. This could be life-threatening for the organizations and especially for their clients.

Developing Composite Client Stories

For many people walking through the door of a independent community service organization, the social services they receive are their lifeline. To illustrate the particular issues facing these clients and the ISCOs which serve them, we have developed three composite sketches of typical clients. These stories are informed by the information gathered at the four site visits and are therefore based on the realities currently faced by ICSOs, but are composite stories so as to not be identifiable as any actual client.

Each story, or case study, sets out the personal situation, needs and concerns of a typical client of the organization in question. The three composite client stories (found in full in Appendices C, D, and E) are:

1. ***Melissa's Story*** – PLEA Community Services operates in the Greater Vancouver area and helps children, youth, adults and families with significant challenges, including youth justice, youth addictions and other residential and support programs. For Melissa, PLEA is a lifeline. Between her first visit in 2005 and the present day (2008), Melissa has accessed PLEA services 24 times, including multiple stays in Detox, the Supported Recovery program, and ONYX Vancouver. She has come to see Lisa, an intake worker with PLEA, to access a Detox program after having previously completed the Daughters & Sisters program. She says she suffers from a learning disability, and has been diagnosed with Hepatitis C. She sometimes lives with a boyfriend who is also an addict. She describes herself as Métis and Christian. She gives Lisa her Care Card Number but does not have a SIN number. Her picture is taken for inclusion with her file… (Read the Melissa composite client story in full in Appendix C.)

2. ***Sam's Story*** – Abbotsford Community Services Society (ACS) operates over 70 programs in Abbotsford and surrounding communities in the Fraser Valley. Sam, 47, has a drug problem. He has bi-polar disorder for which he is on medication. Sam has had a difficult time. He or members of his family have been clients of ACS for many years, meaning there may be several files for Sam given the

different programs he has accessed. Sam is a Ministry of Children and Family Development "mandated" referral by a protection team. After the referral, Sam attends a group orientation at ACS. While there, Sam fills out an orientation form. Sam has a week to call back and when he does an addictions counselor is assigned. Had he not called back all the initial information collected would have been destroyed. But he does. Jerry is assigned as Sam's addictions counselor… (Read the Sam composite client story in full in Appendix D.)

3. ***Bobby's Story*** – Since 1975, several thousand women have come through the doors of Victoria Women's Transition House (VWTH) looking for help, seeking a brighter future for themselves and their children. VWTH provides a safe, welcoming shelter, respectful counseling, support and advocacy. Bobby, 11, is part of the Children Who Witness Violence (CWWV) Program. He has been having trouble in school, and his mother Pam has referred him to the program. Bobby started seeing Jane, his CWWV counselor, in March and started participating in April after school on Wednesdays. Pam and her two kids (Bobby has a six year old sister Caroline) spent 30 days the transition house. She has sole custody of her children, but there are ongoing access-related issues with her ex-husband that are being worked on through the Family Justice Program of the Ministry of the Attorney General… (Read the Bobby composite client story in full in Appendix E.)

As the specific legal research was undertaken, the details of these hypothetical stories were instrumental in playing out the legal issues within a real-life context. As the legal issues are unpacked in the following section, elements of these stories will be referenced. We hope these illustrations will make real the privacy concerns of the clients and the organizations serving them, and provide context for the discussion of the legal issues which will confront them if the proposed ICM system is implemented as planned.

Privacy and the Integrated Case Management System: Unpacking the Legal Issues

Part I: Privacy is a Constitutional Right

The right to privacy is a fundamental right of all individuals in Canada that has been recognized time and time again by the Supreme Court of Canada,

In cases dealing with both sections 7 and 8 of the Canadian Charter of Rights and Freedoms, the Supreme Court has stated that all individuals have a constitutional right of privacy which should be protected as much as is reasonably possible. The Court has also stated that respect for individual privacy is an essential component of what it means to be "free", and any the infringement of this right undeniably impinges upon an individual's "liberty" in our free and democratic society.[27]

The Supreme Court discussed the nature of the right to privacy in decisions under section 8 of the Charter. In R. v. Dyment, Laforest J. advocated a broad, liberal approach to interpreting privacy rights. After reviewing several authorities, Laforest J. stated:

> The foregoing approach is altogether fitting for a constitutional document enshrined at the time when, Westin tells us, society has come to realize that privacy is at the heart of liberty in a modern state: see Alan F. Westin, Privacy and Freedom (1970), pp. 349-50. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[28]

In *Dyment*, Laforest J. also discussed the nature of the right of the privacy, and listed various "zones", or "realms", of privacy, including territorial (property), and personal privacy. He expressly concluded that privacy includes a right to informational privacy:

[27] *R. v. O'Connor*, [1996] 2 W.W.R. 153 at 171 per Lamer, at 207 per L'heureux Dube at 207
[28] *R. v. Dyment*, [1988] 2 S.C.R. 417

> Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force [from Privacy and Computers, Report of the Task Force established by the Departments of Communication and Justice (1972)] put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the Privacy Act, S.C. 1980-81-82-83, c. 111.

La Forest J. concluded that when balancing the rights of the individual with those of the state, care must be taken to ensure that the individual's right to privacy is violated as little as possible.

In *Dagg*, Laforest J. then repeated the statement from Dyment referred to above, and indicated that the right to privacy includes the right of control over knowledge about oneself:

> See also R. v. Duarte, [1990] 1 S.C.R. 30, at p. 46 ("privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself"); R. v. Osolin, [1993] 4 S.C.R. 595, at pp. 613-15 (per L'Heureux-Dubé J., dissenting); Westin, supra, at p. 7 ("[p]rivacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others"); Charles Fried, "Privacy" (1968), 77 Yale L.J. 475, at p. 483 ("[p]rivacy . . . is control over knowledge about oneself").
>
> Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R. 403

In short, the Supreme Court of Canada has ruled that the Constitution protects "a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[29] [Emphasis added.]

Many of the Court's decisions involving the right of privacy turn on section 1 of the Charter which provides that all Charter rights are subject to "reasonable limits that can be justified in a free and democratic society". In other words, where privacy has been breached it is up to the government to justify the breach in accordance with the exacting standards required pursuant to *R. v. Oakes*, [1986] 1 S.C.R. 103. A detailed reviewe of the Oakes test is beyond the scope of this report, but generally section 1 requires a delicate balancing of the individual's right to privacy with the government's stated

[29] *R.* v. *Plant*,[1993] S.C.J. No. 97 (Q.L.), para. 19.

objective. The Court will carefully scrutinize the government's objective and also require that the governments demonstrate that the breach of privacy was the least intrusive means of furthering the objective.

In this regard, FIPPA provides that a disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

(a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation[30].

It is far from clear that the massive invasion of individuals' privacy contemplated by the ICM is consistent with the right of privacy articulated by Canadian courts.

Recommendation: The BC government should draft a constitutional question regarding the proposed ICM system and refer the matter to the BC Supreme Court pursuant to the Constitutional Question Act, RSBC 1996, c. 68, for an opinion on its constitutionality.

Part II: Privacy Legislation

1. Introduction

The right to privacy is embodied in federal and provincial legislation.

In BC, privacy is governed by two main statutes: the *Personal Information Protection Act* which applies to the private and non-profit sectors and the *Freedom of Information and Protection of Privacy Act* which applies to the provincial government, municipal bodies and other government entities such as health authorities, hospitals and professional regulatory bodies.

Both statutes create rules governing the collection, use, disclosure and security of personal information. The rules are based largely on the ten core principles for protection of privacy originally developed by the OECD and now widely recognized throughout the world as the basis for privacy protection. [31]

2. Consent

Consent is the cornerstone of any privacy policy. The principle of consent is how society has decided to protect client confidentiality. Privacy without a right of consent is meaningless. The federal Privacy Commissioner has described informed consent as "the backbone of our net of privacy principles and practice – the glue that holds the fair

[30] *FIPPA, supra* note 17 at s. 22 (3)
[31] OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

information principles together. . . . In turn, confidentiality refers to a duty that one owes to safeguard information that has been entrusted to them by another. . . In the health care context, care providers have confidentiality duties in regard to their patients that are founded on and emphasized both by ethical and legal principles[32]

Under PIPA, an individual's consent is required for the collection, use or disclosure of personal information. Although PIPA provides that an individual's consent can be implied in certain circumstances, implied consent must be informed, and the individual provided with sufficient information about the proposed collection, use or disclosure to enable them to make meaningful decisions about their personal information. Generally, for implied consent to be truly voluntary an individual must be informed about their right to expressly withhold or withdraw consent at any time. Consent, to be validly given, must be voluntary and informed.[33] Informed consent is the requirement to ensure that the client understands what they are consenting to.[34]

In contrast, FIPPA does not require individual consent and information can be shared broadly within government. FIPPA permits collection of personal information when it is:

(i) authorized by statute;

(ii) done for law enforcement purposes; or

(iii) the information "relates directly to and is necessary for an operating program or activity of the public body".

The latter standard in particular permits widespread disclosure without individual consent.

Presently, ICSOs are required to obtain individual consent to collect, use or disclose personal information. However, the ICM contemplates all such personal information being transferred to the provincial government. Thus, the effect of the ICM is to apply the less rigorous standard of FIPPA to non-governmental organizations thus circumventing PIPA's individual consent requirement. As a result, any individual seeking out the services of an ICSO loses the fundamental right to control their own personal information.

3. Collection

There is no indication that the collection of information contemplated by the ICM has been authorized by statute or is being done for a done for law enforcement purposes. Therefore, it is important to consider the whether the collection can be justified as being "related directly to and is necessary for an operating program or activity of the public body".

---

[32] Address by Jennifer Stoddart, Privacy Commissioner of Canada, *Privacy Laws & Health Information: Making it Work*, presented at Privacy Laws & Health Information Conference, October 27, 2004, Regina, Saskatchewan. Text of address available online at: http://www.privcom.gc.ca/speech/2004/sp-d_041027_e.asp ["Stoddart Address"].

[33] *FIPPA and PIPA, supra* note 17.

[34] The progress of informed consent in the medical context has been documented by Bernard Dickens and Rebecca Cook. See: Dickens, B.M. and R.J. Cook, "Dimensions of Informed Consent to Treatment" (2004) 85 International Journal of Gynecology and Obstetrics 309, and Dickens, B.M. and R.J. Cook, "Law and Ethics in Conflict Over Confidentiality?" (2000) 70 International Journal of Gynecology and Obstetrics 385.

The legal environment within which the proposed ICM functions is significant. A brief review of the legislative framework indicates the breadth of information that may be collected by Government pursuant to statute.[35] MHSD and MCFD both collect a huge array of information. For example, Sections 10 and 11 of the *Employment and Assistance Act* and similar provisions in its sister *Employment and Assistance for Persons with Disabilities Act*, specify the kinds of information that can be collected and the purposes of the collection[36]. MCFD collects information under 10 different statutes[37]. Each statutory regime enables the collection of different sorts of information.

In most of the cases that we reviewed, the ICSOs do not establish eligibility for programs under statute nor do they collect information pursuant to these statutory mandates[38].

Several decisions of the Information and Privacy Commissioner and the Courts have clarified what is 'necessary collection' for the purposes of FIPPA. In F07-10, the OIPC states[39]:

> The following complete quote from the Black's Law Dictionary (6th ed.) definition of "necessary" emphasizes the contextual malleability of "necessary", a word that is fairly common in statutes:
>
> > This word must be considered in the connection in which it is used, as it is a word susceptible of various meanings. It may import absolute physical necessity or inevitability, or it may import that which is only convenient, useful, appropriate, suitable, proper, or conducive to the end sought. It is an adjective expressing degrees, and may express mere convenience or that which is indispensable or an absolute physical necessity. It may mean something which in the accomplishment of a given object cannot be dispensed with, or it may mean something reasonably useful and proper, and of greater or lesser benefit or convenience, and its force and meaning must be determined with relation to the particular object sought. . . .
>
> …The collection of personal information by state actors covered by *FIPPA*—including local public bodies such as the Board—will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of *FIPPA*. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.[40]

---

[35] This information is contained on one of the Appendices to the RFP (*supra* note 3).
[36] *Employment and Assistance Act,* S.B.C. 2002, c. 40
[37] *RFP, supra* note 7 at para. 3.2.3
[38] The exceptions to this might be those be those under the Community Living BC rubric where the regulations are quite specific about the care to be afforded to individuals. However, as extensive human rights jurisprudence demonstrates, care of people with disabilities is largely left to individuals.
[39] Office of the Information and Privacy Commissioner, "Order F07-10: The Board of Education of School District No. 75 (Mission)" at paras. 40-48.
[40] *Ibid.* at paras. 40-48.

The collection of client information is necessary for ICSOs to meet their mandates. It is not obvious how the collection of additional personal information by government is necessary, since they have not in the past required the amount of personal information they are now demanding. Most ICSOs provide extensive reporting of aggregate and demographic data to satisfy the government. Few would question the need for government to review such data to ensure public funds are being properly spent within the agreed parameters, and are being used efficiently and effectively. However, this legitimate purpose does not require access to individual, personal information. It is unlikely that such collection would be upheld based on the criteria set out by the Information and Privacy Commissioner and the courts.

Recent court cases reviewing the purposes of collection of information from second hand goods sellers offer further support for this view. In the *Cash Converters*[41] case, the Ontario Court of Appeal was asked to consider a municipal by-law requiring second hand goods dealers to provide a daily record containing personal information of sellers. While the court upheld the by-law in so far as it met the requirement of consumer protection under the division of powers, it found that the requirements for the provision of information were not necessary within the meaning of the *Municipal Freedom of Information Act*[42]. The Court found:

> The effect of this evidence is that the new provisions are intended to improve the old system by modernizing the recording of the information using computers and by making the system easier for the police to administer because they receive the information electronically on a daily basis without travelling to the second-hand stores. However, it is clear that there is no attempt to say that the new provisions are necessary for administering the licensing system or for its effectiveness. In contrast, in the *Toronto Taxi Alliance v. City of Toronto*, [2005] O.J. No. 5460 (C.A.) the city had two task force reports that discussed the problem with taxi licenses and how the new by-law would address the problem. . . .
>
> The effect of the new by-law is to facilitate the collection and electronic recording of detailed, identifying information about persons, mostly innocent but some unscrupulous, including their photograph and details of three pieces of identification as well as the time of their visit to the store and the nature of the goods offered for sale. This information is then transmitted and stored in a police database and available for use and transmission by the police without any restriction and without any judicial oversight. The intent of *MFIPPA* is to ensure that the collection and retention of private information is strictly controlled and justified.
>
> Based on the evidence in this application, the city has not demonstrated that the impugned provisions of the new by-law that mandate the collection and electronic transmission to police of detailed personal information about vendors of second-hand goods, is necessary for an effective consumer protection regime to license

[41] *Cash Converters Canada Inc. v Oshawa (City*), 86 O.R. (3d) 401 (Ont. C.A.) A similar New Westminster bylaw was struck down on administrative law grounds in *Royal City Jewellers & Loans Ltd. v. New Westminster (City)*, 2007 BCCA 398.

[42] *Municipal Freedom of Information and Protection of Privacy Act,* R.S.O. 1990, c. M.56.

> second-hand dealers. Given my conclusions that the impugned provisions in the new by-law do not come within the exceptions in s. 28(2) of *MFIPPA*, I am of the view that the application judge erred in law in his application of the Rothman's test.
>
> In this application, the city effectively took an "all or nothing approach" to the by-law, and did not seek to justify the provisions clause by clause. As a result, I would declare the challenged sections of Schedule A to the by-law: ss.10(c), (d), 15, 20, 22 (a), and (b) to be "of no effect" under s. 14 of the *Municipal Act*, 2001.[43]

The Court's reasoning is consistent with that adopted by BC's Information and Privacy Commissioner in deciding that broad enabling legislation is not sufficient to cover the collection of personal information unless the collection is necessary to the function of a particular program. Whatever business outcomes the contract contemplates, the actual outcomes are those entirely determined by the client and the ICSO. The information that is collected from a client belongs to her and while she is working with an ICSO, ought to remain entirely within the custody and control of that organization.

An interesting court decision regarding collection of personal information by government is the *Patterson*[44] case. In Patterson, income assistance applicants brought a *Charte*r challenge to mandatory consent to release third party financial information required of social assistance applicants. While the majority of the BC Court of Appeal upheld the constitutionality of the broad language on the basis that it was only being used to verify personal information that had already been supplied by the applicant, Madam Justice Ryan disagreed, and issued a strong dissent:

> The right to privacy was a principle of fundamental justice recognized in s. 7 of the *Charter*. The state had a valid interest in verifying personal information upon which applications for social assistance were based, but the consent form in question was not limited to such verification. The language of the consent permitted a standardless sweep by allowing government officials to pursue their own predilections in determining what information might be relevant to an applicant's eligibility for benefits. By allowing government employees and custodians of applicants' records to determine what information was relevant, the consent put applicants' personal information at risk of indiscriminate disclosure[45].

It is important to note that the applicants in Patterson did not raise the possible application of FIPPA and the rigorous standard for collection of personal information.

It is also important to note that the majority upheld the broad consent on the basis that it would verify already disclosed information. The proposed ICM system is ambiguous on this point, indicating that ICSOs would be required to routinely provide the government with an array of personal information, but leaving the purpose for the collection of this

---

[43] *Cash Converters, supra* note 41 at paras. 49-53.
[44] *Patterson v. British Columbia (Ministry of Human Resources),* [2000] 181 D.L.R. (4th) 193 (B.C. C.A. Nov 10, 1999) Leave to appeal to SCC refused.
[45] *Ibid*. at para. *27*

information either unstated or stated in very general terms related to overall functioning of the system, rather than to a purpose related to the client.[46]

Based on our review and research, Madam Justice Ryan's concern about unfettered discretion in the hands of government officials is not misplaced. Her concern ought to give us all pause when we consider the extent to which we have already given various bodies seemingly broad powers to access information without specific and informed consent. Unless disclosure is mandated, and the person who supplies the information has given their informed consent, the agency ought not to disclose the personal information.

Given that the government has not required personal information from ICSOs and there is no evidence that the current system is affecting the ability of ICSOs to provide services, it seems difficult to suggest that widespread collection of personal information through the ICM system is "necessary for for an operating program or activity" of the government.

Surely the government ought to be called upon to fully justify the necessity of the widespread collection contemplated by the ICM and to provide specific and detailed evidence that requiring ICSOs to provide all of their client's personal information is necessary.

Part III: Confidentiality and Therapeutic Relationships

Social service providers must be able to ensure confidentiality in order to establish the trust and confidence of individuals seeking assistance.

The following excerpt from the BC Physician Privacy Toolkit (2nd edition – June 15, 2009) (a joint project of the British Columbia Medical Association, the College of Physicians and Surgeons of British Columbia and the Office of the Information and Privacy Commissioner), underscores the importance of confidentiality to effective health care:

> Health Information is one of the most sensitive forms of personal information.
>
> Both privacy and security of personal health information are major concerns for physicians because both are fundamental to the confidentiality and trust of the physician-patient relationship. If patients do not have the confidence that their privacy will be maintained, or that reasonable security safeguards will be in place to protect their information, they may do things to protect their privacy on their own (such as refrain from disclosing critical information, refuse to provide consent to use personal health information for research purposes, or not seek treatment). Such behaviour was illustrated in a 1999 Canadian Medical Association (CMA) survey, which found that 11% of the public held back information from a health care provider due to concerns about whom it would be shared with or what purposes it would be used for.

[46] See 2007 RFP paras 6.3.1 (Business Function Requirements)and 6.3.7 (SDP Requirements) See also SATP-270, February 5, 2009 p.50-51

Protecting the confidentiality of information is a fundamental principle underlying the community and social service sector.

> Privacy of personal information goes to the heart of our identity as human beings and is fundamental to a person's dignity, integrity and autonomy. Privacy is necessary for health. An individual's sense of identity, dignity, self-esteem, competence and personal choice are recognized as critical elements within the principles of psychosocial rehabilitation and recovery.
>
> However, self-disclosure is also linked to mental health, and the expectation of confidentiality in the therapeutic relationship can open the way for willing disclosure of sensitive personal health information. . . . Providers believe that if clients do not trust that their personal health information will be protected, they will be reluctant to fully and honestly share personal health details and may avoid seeking care altogether[47].

The US Supreme Court recognized the importance of confidentiality when it asserted the psychotherapeutic privilege in *Redmond*:

> The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance. [10] … As we explained in *Upjohn*, if the purpose of the privilege is to be served, the participants in the confidential conversation "must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.[48]

The language of the US Supreme Court in *Redmond* is mirrored in privacy legislation where there is acknowledgment of the damage that can be done when there is unauthorized disclosure of sensitive personal information, particularly of a medical or psychological nature.

---

[47] Goldner, Elliot M., Judith Tompkins, and Karen Cardiff, "Mental Health On-line: A Case for Information Management", final report made to Health Transition Fund, Health Canada February 2001, [Mental Health On-line] at pp. 25-26. See also: Anderson, Ross, "Patient confidentiality and central databases" British Journal of General Practice, Volume 58, Number 547, 1 February 2008, pp. 75-76(2), Linzer, N., A. Conboy, and E. Ain "Confidentiality: An Ethical Dilemma for Israeli Social Workers" (2004) 3 Journal of Religion and Spirituality in Social Work 85. "Without confidentiality, there can be no trust between the client and the professional. Violations of confidentiality threaten therapeutic relationships." Gelman, Sheldon R., Daniel Pollack, and Adele Weiner, "Confidentiality of Social Work Records in the Computer Age" (1999) 44 Social Work 243.

[48] *Jaffee v. Redmond,* 518 U.S. 1 (1996) (U.S.S.C.) at para. 449. The Court notes that state statues extend the privilege to psychiatrists and psychologists, while most apply the protection more broadly. "behavioral health professionals" . . . to persons "licensed or certified by the State of Texas in the diagnosis, evaluation or treatment of any mental or emotional disorder" or "involved in the treatment or examination of drug abusers" and "marriage and family therapists, professional counselors, and psychiatric mental health nurse specialists".

Section 22(3)(a) of FIPPA presumes that the release of personal information relating to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation is an unreasonable invasion of personal privacy.

The Integrated Case Management system creates enormous risks that therapeutic relationships will be undermined.

Many community and social service providers are concerned about the impact of disclosure of information to government. Some verbatim comments received include the following:

- "We think private client information should not be disclosed to government. It is our practice that we do not"
- "Tension exists between our role as advocates and as contractors . . ."
- "Clients would be less likely to disclose personal information to us"
- "The majority of clients do not realize the privacy implications and just sign. Other clients are very paranoid and won't provide information. We still provide services"
- "Some people refuse service"
- "Clients feel less trust and sometimes hold back important information"
- " . . . I needed to comment that we would opt out of providing the service should this become an issue"
- "Young people are more suspicious of the service, less open, less trust"
- "I believe the only time we might have to disclose client file info to government would be in the case of a child protection issue. For mothers, our requirement to report and/or our requirement to provide information may cause them to feel insecure about accessing our services and/or about telling us everything they need to/want to tell us"

The MCFD holds information in its Management Information System (MIS) database. The database contains all the information ever gathered by the MCFD about the tens of thousands of families that have come in contact with the Ministry at various points in their lives. It holds information about children in need of a protection. It also includes information about licensed child care providers, foster parents, providers of home nursing help, palliative care in the community, and may include extensive information about the many people in the community who come into contact with those individuals including doctors, nurses, psychologists and other care and social support providers. In short, some information will be found in the MIS (or another similar) system if anyone has ever had contact with a licensed daycare provider, a parenting group, a Mom and Me baby group, or needed family counseling to get through a rough patch often without the knowledge or consent of the person concerned.[49] This particular MIS is only one of the hundreds of databases the government maintains that hold the stories of many of our lives.

The policy of MCFD with respect to its MIS is to hold on to the information in perpetuity. As illustrated by Sam's situation, much of the information in Sam's file contains assertions and self-disclosures about the extent of his drug use that are clinically irrelevant, yet could follow him for the rest of his life.

[49] In *Bracken v. Vancouver Police Board*, [2006] B.C.W.L.D. 2505 (B.C. S.C.), an individual complained about the significant amount of personal information contained in databases held by the MEIA and disclosure without consent.

For clients who access several services provided by different programs at ACS and potentially linked to funding from several Ministries including MEIA, MCFD and Ministry of Health, the failure to maintain confidences could have far-reaching implications. Our stakeholder survey suggested that failure to maintain client confidences could severely affect access and referrals to many community social services. Our research indicates that clients will refuse to access the services they need if their confidentiality is not assured.

The mental health and well-being of an individual should be considered when any disclosure is contemplated. We would contend that no matter what service is offered to the individual, whether explicitly psychological or a social support necessary to promote their mental well-being, all such information ought to be treated as confidential. Without such assurances of confidentiality, an individual may decide not to access services, a decision which could be life-threatening. This view is consistent also with several court decisions which considered the potential prejudice and damage to individuals' mental health where disclosure of information is sought. In the *Osolin* case, the court was asked to consider the potential disclosure of an abuse victim's diary to defence counsel. The Court found that:

> . . . medical records concerning statements made in the course of therapy are both hearsay and inherently problematic as regards reliability . . . . . in therapy an entire spectrum of factors such as personal history, thoughts, emotions as well as particular acts may inform the dialogue between therapist and patient. Thus, there is serious risk that such statements could be taken piecemeal out of the context in which they were made to provide a foundation for entirely unwarranted inferences by the trier of fact.[50]

Micheal Vonn, in her recent article, "The Real Impact of the E-Health Act" stated:

> Patients' loss of control over disclosures of their data in a centralized electronic health records erodes trust in health care and creates formidable barriers to access. Two years ago, a Scottish study showed that 25 per cent of people were less likely to attend sexual health clinics if the records were shared in electronic databases, and almost half of the study participants didn't even want their GPs to have access to their sexual health information on a shared electronic database. The Royal College of Physicians and Surgeons in the United Kingdom, a country that was an early adopter of centralization electronic health records, recently reported that a staggering 79 per cent of over 3,500 surveyed physicians would not seek mental health treatment from the local National Health Service, the majority citing concerns about medical confidentiality.[51]

The need for trust and mutual respect in the relationship between counsellors and clients is deeply embedded in our culture and laws. A project like the ICM system, which has a significant potential to undermine the confidential nature of such relationships, ought to be subjected tot he highest scrutiny.

---

[50] *R. v. Osolin* (December 16, 1993), 22826, at p. 19 [reported 26 C.R. (4th) 1, at pp. 63-64] See also V (K.L. v. R(D.G) [1994] 95 B.C.L.R. (2d).

[51] The Advocate, Vol.67, Part 6, November 2009, pp.753-758

Recommendation: The government should conduct social policy research including surveys to determine the impact of the ICM system on citizen's willingness to seek out the services they need.

Part IV: Privacy, Technology and Security

In his 2007-08 Annual Report, Information and Privacy Commissioner David Loukidelis expressed concern for the lack of awareness on the part of public bodies and organizations of "the weaknesses of their technical and administrative information security. This is bad for privacy. This is also bad news for the security of government or corporate information assets."[52]

The Commissioner also advised that his office had investigated 96 privacy breaches including 10 from one Ministry alone[53].

> Finally, security refers to measures taken to safeguard personal information from unauthorized access, use or disclosure. Some distinguish between data security and system security. Data security results from measures that effectively protect data and computer programs from threats such as: unauthorized access and disclosure; impermissible alteration; unauthorized copying; theft; loss due to system failures or operating error; and physical damage (caused by fire or flood, for example). . . . In contrast, system security refers to the sum of all measures in place – including technological measures aimed at data security, personnel policies, practices for monitoring compliance, and so on – that are aimed at protecting personal information[54].

While the principles of security may be well understood, it appears that their application in practice leaves something to be desired. Ministry budgets allocate millions of dollars for records management and information security. Notwithstanding these millions, security breaches occur:

- Unencrypted magnetic tapes were lost between New Brunswick and B.C. despite policies in place to ensure encryption, and it appears some Ministries have not followed existing guidelines and policies.
- When closing the MHSD (when it was MEIA) office in Burnaby several boxes of disks and tape containing sensitive personal information were mislaid and, subsequently apparently purchased at a government auction.

---

[52] Office of the Information and Privacy Commissioner for British Columbia, Annual Report 2007-2008 (July, 2008).
[53] Ibid.
[54] University of Alberta (Health Law Institute) and University of Victoria (School of Health Information Science) "Electronic Health Records and the *Personal Information Protection and Electronic Documents Act*" April 2005, at p. 15.

- In his report on the CORNET system, the Auditor General was so alarmed by breaches to security that he took action while the investigation was ongoing to ensure the breaches would cease.[55]
- Earlier this year, the Acting Commissioner issued a damning investigation report[56] about a breach at the MCFD and MHSD involving the records of more than1400 clients. The Commissioner highlighted the lack of knowledge of privacy rules within the ministries, and called executive leadership on the carpet for this and other failures.

These breaches are occurring despite a purportedly robust information security environment. Our review of privacy decisions by the OIPC documents the ongoing concern and extent of breaches to security of information[57].

The situation for non-profit organizations which do not have the benefit of millions of dollars for equipment and IT staff is even more serious.

In our stakeholder survey only 26.5% of respondents indicated that they had "very adequate resources" to allocate towards privacy and security issues. A great many (44.1%) do not think they have adequate resources to address existing requirements, let alone new demands:

- "Privacy functions are considered to be assumed by the organization. Funders are not interested in funding such initiatives and assume organizations are completing privacy audits."
- "We dedicate adequate resources [to privacy] but we don't receive adequate resources to meet the expectations from our funders, accrediting bodies and our own professional standards."

Notwithstanding their financial shortcomings, many ICSOs have put in place elaborate manual systems to protect their clients' sensitive personal information. These manual systems are not perfect, but they are workable in the context of small community organizations. Of the four agencies visited, only one had full access and encryption software.

The imposition of a complex electronic system on a sector without taking account of the systems and mechanisms currently in place and resources available for new systems poses real potential for failure.

---

[55] CORNET is the database holding all the information within the correctional system. It and JUSTIN are probably among the most sensitive information databases held by the Province. Office of the Auditor General, Managing access to the corrections case management system 2008.

[56] F10-01 February 8, 2010. [2010] B.C.I.P.C.D. No. 3

[57] Office of the Information and Privacy Commissioner "Investigation Report 01-01- Investigation into BC Nurses' Union Complaint about Telus-VGH LastWord Contract" October 5, 2001, at para. 97. See also Office of the Information and Privacy Commissioner "Order P06-04-Twentieth Century Fox Film Corporation" October 26, 2006, at para. 80, and Office of the Information and Privacy Commissioner "Order F06-01- Ministry of Energy, Mines and Petroleum Resources" at paras. 49-50.

When our survey asked whether there was additional funding available to handle the information management and records retention requirements in their contractual arrangements with their funders, most agencies said no. This is a critical resource issue.

The RFP for the ICM system requires successful proponents to "provide comprehensive roles-based security features to meet control and privacy concerns for users and ensure protection of operational data."[58] These systems presumably are to be consistent with the Office of the Chief Information Officer's security policies, privacy legislation and the province's authentication infrastructure[59]. The proposed ICM system will "manage and maintain the appropriate levels of access to information and functions using the system's internal security functionality."[60] This functionality will be built on an Information Access Layer (IAL) which itself will be built upon the Health Information Access Layer (HIAL) system currently being created for the provincial Government's eHealth information sharing project.

This planned integration through the IAL includes:

- client identity and access management,
- service provider identity,
- guidelines for release or masking of data in the system,
- common audit and logging,
- secure messaging, notification and delivery of message payloads[61].

At a recent discussion with the Chief Information Officer of the Province of BC, among others, it appeared the underlying assumption was that the current levels of security were adequate to the task presented by IAL/HIAL.

The system as we understand it will rely on individual agents and agencies to follow the appropriate safeguards to ensure the security of information. This reliance on security causes the social service sector some concern because:

- there are no unified security standards in place across the sector, and
- the sector lacks the resources to implement the kinds of electronic security that would be necessary to make the system work securely.

Without significant additional resources to address these issues, we are concerned about the ability of agencies to protect client privacy if the ICM system is introduced in its current form.

Recommendation: The Government must immediately assess the resources available to the service delivery providers to ensure that proposed clients and users of the ICM system have the necessary resources, education and training necessary to implement the ICM system. The Government must ensure that proper resources and training are available prior to implementation.

[58] RFP, *supra* note 7, Appendix L at p.5. See also **SATP-270, February 5, 2009 p.42**
[59] RFP, *supra* note 7 at p. 36. See also **SATP-270, February 5, 2009 p.42-44**
[60] RFP, *supra* note 7 at p. 37. See also **SATP-270, February 5, 2009 p.42-44**
[61] RFP, *supra* note 7 at p. 38. See also **SATP-270, February 5, 2009 p.29**

PART V: The Role of the Information and Privacy Commissioner

(i) Privacy and Health information Technology

In a 2001 paper[62], the Information and Privacy Commissioner outlined the privacy challenges created by information technology in the health sector:

> The OIPC must continue to rely on the positive relationships it has developed with various health care bodies. New challenges are emerging and, with our emphasis on communication at the start-up phase of a project and as an on-going tool, privacy can be better protected only with ongoing dialogue.
>
> Two new challenges have already identified themselves. Continuing regionalization indicates that even more layers of privacy safeguards will be needed, as more people will have access to data. In addition, administrative teams will need to ensure safeguards are in place and that staff are adequately trained.
>
> Information technology can pose a great threat to personal privacy. The health sector in public body is quickly moving towards an Internet-based records management system that would allow for information-sharing among a variety of healthcare workers and agencies. The HealthNet/BC system is attempting to connect all healthcare workers in order to facilitate data transfers. The privacy implications are notable and, with the OIPC's support, the Ministry of Health has already taken a number of steps to ensure some privacy protection. These measures include:
>
> - providing free software – called HN Secure – to all doctors, pharmacies and labs, to help them ensure the secure transfer of data over the Internet,
> - implementing training requirements for anyone who will be using the integrated electronic system,
> - restrictions on who can access the system to those who need access to the data for work purposes, and
> - creating doctor's office information brochures for patients entered in the system.
>
> There is little doubt that more work is required in order to ensure health information privacy. Each project provides more knowledge about how to work together and achieve the mutually beneficial results of quality patient care and protection of patients' fundamental rights. The interaction of privacy experts and health experts is an essential component of this. The continued development of strong relationships between the OIPC and health care bodies will help ensure that health privacy remains an important issue during both the implementation and on-going phase of various projects.

---

[62] *HEALTH INFORMATION PRIVACY – THE BRITISH COLUMBIA EXPERIENCE,* Canadian Institute Conference – David Loukidelis, Information and Privacy Commissioner of BC, June 19, 2001

The largest issue of all, of course, is how ongoing federally-funded harmonization initiatives will play out. Thus far, British Columbia has decided that one Act is enough to protect health information, but enactment of the *Personal Information Protection and Electronic Documents Act* and initiatives under the Health Infoway (for example) raise the question of where harmonization will take us. To the lowest common denominator?

There is no indication that the government has engaged the Office of the Information and Privacy Commissioner. Given the privacy issues at stake, this is a huge oversight.

Ann Cavoukian, the Information and Privacy Commissioner of Ontario has written extensively on the importance of addressing protection of personal privacy by embedding privacy principles into the systems development process at the earliest possible time[63].

Privacy by Design

Privacy by Design (PbD) is a concept developed by Dr. Ann Cavoukian, in the mid-nineties. In brief, PbD is a concept that involves embedding privacy into the design specifications of technologies. This process begins by building the principles of Fair Information Practices (FIPs, see Appendix A) into the design, operation and management of information processing technologies and systems, and then elaborates them to the gold standard of becoming the default. While PbD has information technology as its primary area of application, it has since expanded in scope to include two other areas. In total, the three areas of application are: (1) information technology; (2) accountable business practices; and (3) physical design and networked infrastructure. The current era is one of near-exponential growth in the creation, dissemination, use and retention of personally identifiable information. Whether applied at the level of information technology, business practices or systems, it is more critical now than ever to embrace the *Privacy by Design* approach if privacy, as it is currently known, is to survive well into the 21st century.

(ii) Privacy Impact Assessments

Section 69 of FIPPA provides that Ministries undertaking a new information-sharing system, project or program must carry out a privacy impact assessment. A privacy impact assessment ("PIA") is defined in section 69 as follows:

> "[P]rivacy impact assessment" means an assessment that is conducted to determine if a new enactment, system, project or program meets the requirements of Part 3 of this Act.

Subsection 69(5) of FIPPA states:

[63] Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design November 2009

> 69(5) The head of a ministry must conduct a privacy impact assessment and prepare an information-sharing agreement in accordance with the directions of the minister responsible for this Act.

The Commissioner has described PIAs as follows:

> Unlike the examples of cooperation in the form of the PharmaNet initiative and the model bylaws, use of a privacy impact assessment tool ("PIA") is an initiative of the OIPC. Our PIA tool – which is under revision - has the broadest possible application. This self-administered assessment is designed for use by all public bodies, regardless of their mandate or size, to identify and avoid (or mitigate) the impact on privacy of any proposed laws, programs or policies. We have continually urged all public bodies to use the PIA tool at the earliest possible stages of design, to ensure that inappropriate proposals are identified and killed, or amended, before it becomes too costly to do so. (Our model PIA tool – which is found on our website – is in the course of being revised in light of recent developments generally in privacy practices.)
>
> PIAs are an invaluable resource, especially, for policy-makers or planners who are new to the world of privacy protection. By laying out a number of significant issues – including nature, source, use, disclosure and security of information collected – as well as examining the individuals affected and the authorization of and notification for collection, PIAs help to avoid privacy violations. Perhaps one of the greatest dangers associated with them, however, is the tendency to regard a PIA as a merely a managerial tool – one that identifies and manages privacy impacts, rather than identifies them and avoids them altogether.
>
> PIAs illustrate a challenge that faces regulatory bodies such as the OIPC – ensuring that regulated parties are reminded of and are knowledgeable about, their legal duties. In the case of the PIA tool, placing it on our website is one way of advocating its use, but it is not the only (or best) way to ensure it is used. As a result, neither I nor my colleagues miss an opportunity to urge public bodies to use PIAs, wherever possible, and to suggest that they provide us with a copy of PIAs for comment and feedback (though not formal approval of proposed actions). We do this through speeches, meetings, letters, our newsletter and word of mouth. This is a good example of how regulatory bodies such as ours must use education, advocacy and persuasion to ensure the spirit and letter of the law are well known and are acted on. [64]

The proposed ICM system may be the most intrusive invasion of client privacy ever by a BC government. Based on the information available about the system, it does not appear that important issues such as individual consent, necessity of collection, and security of information have been adequately addressed in the design of the system. These are significant issues that must be addressed at the outset of the design of this new information management tool. It will be difficult if not impossible to address these issues after the system is designed and implemented.

[64] Ibid.

The ICM has the potential to be vastly over-reaching, amounting to collection, use and potential disclosure of information inconsistent with existing privacy law and practice. If not already done and referred to the Information and Privacy Commissioner, a privacy impact assessment should be carried out immediately.

Recommendation: The government must carry out a privacy impact assessment and refer the ICM project to the Information and Privacy Commissioner to ensure that the ICM system is developed in accordance with existing laws and that protection of individual privacy is built into any system at the outset.

Conclusions and Recommendations

Conclusions

Over the course of this research project we have learned a lot about the complex and shifting landscape within which independent community service organizations are working. We have learned that most ICSOs are very confused by the myriad issues presented by agreements with varying levels of government and a patchwork approach to privacy.

Technology is not a panacea that will solve the challenges facing ICSOs. Technology ought to be an aid to ensure that the values of privacy, confidentiality and autonomy are respected by all. Those who have an interest in the provision of care and social support cannot count on there being more security in the proposed ICM system than is currently in place.

It is our conclusion that the confusion, overlapping interests and patchwork approach to these issues present serious problems that need to be resolved before beginning development of an ICM system.

It is in the interests of all to ensure that whatever future system is designed, it is a system that truly ensures ethical and legal clarity for clients, contracted service organizations and governments.

Recommendations

There are five sets of recommendations below, one set for clients, one set for ICSOs, and one set for the provincial Government.

Recommendations to government

1. Refer to the BC Supreme Court

   The BC government should draft a constitutional question regarding the proposed ICM system and refer the matter to the BC Supreme Court pursuant to the Constitutional Question Act, RSBC 1996, c. 68, for an opinion on its constitutionality.

2. Conduct social policy research

   The government should conduct social policy research, including public opinion surveys, to determine the impact of the ICM system on citizens' willingness to seek out the services they need.

3. Carry out a privacy impact assessment

   The government must carry out a privacy impact assessment and refer the ICM project to the Information and Privacy Commissioner to ensure that the ICM system is developed in accordance with existing laws and that protection of individual privacy is built into any system at the outset.

4. Make appropriate resources available

   If a final decision is made to proceed with the ICM system, the government must immediately assess the resources available to the independent community service sector to ensure that proposed clients and users of the system have the necessary resources, education and training necessary to implement it. The government must ensure that proper resources and training are available prior to implementation.

Recommendations to clients

5. Expect commitment to ethical/legal standards

   Clients must be informed of their privacy rights in a manner appropriate to their circumstances that permits and encourages them to exercise those rights. They must expect and demand the highest legal and ethical standards regarding privacy, confidentiality and consent from ICSOs.

   - Privacy standards need to be clearly delineated, explained and enforced.
   - Clients must be able to expect that confidential relationships with staff will remain confidential within the law.

6. Expect systems that respond to client needs

Working in the interest of clients means going beyond the default positions related to privacy:

- Clients must be in a position to request referrals and transfers of personal information in order to achieve best results for themselves, rather than being put in the position of having to deny consent for information sharing.
- Clients must have the right to 'opt in' to information sharing on an as-required basis rather than having to 'opt out' of pre-ordained information sharing regimes with which they disagree.
- Clients must be able to understand and approve information-sharing arrangements at the commencement of services. When service is provided by a team or multiple providers who work together, information sharing should be limited to "need to know" and the client must have the right, within the law, to impose additional limitations.
- Where service providers are using client information for evaluation or research purposes, clients must be able to expect that strict controls have been established to ensure that data is stripped of individual identification, and that appropriate ethics reviews are conducted and approvals are obtained.

Recommendations to Colleagues in the Community Service Sector

7. Obligations under Law/Obligations under Contracts

The primary legal obligations of ICSOs as defined under PIPA cannot be circumvented in consequence of actions or decisions by any external source, including government. ICSOs contracted to perform work for a government are not "agents" of the crown, and the FIPPA requirements faced by government are not somehow transferable to ICSOs in such a way that they vitiate or obviate PIPA requirements. For government to attempt to impose FIPPA requirements onto community organizations through contract language is legally problematic, especially if and where the government seeks to impose FIPPA requirements as a means of "trumping" and thus avoiding the PIPA requirements to which the organizations are subject.

The basic premises must be that:

- ICSOs must not share personal information held by the organization without appropriate consent, no matter what is provided in their contracts with government funders. The only exception to this position ought to be where disclosure is required by law or court order;
- Where there is such a legal requirement to share information, it should only be shared to the extent permitted by the relevant applicable statutes.
- Contracts should be vetted to ensure compliance with PIPA.

8. New information framework required

A new framework and consequent basic set of policies and procedures need to be developed that ensures the protection of clients, staff and the officers and directors of ICSOs.

a. The framework needs to provide clarity, in common language, regarding the application of PIPA and the requirements it imposes on community organizations (as distinct from the FIPPA requirements for governments and public bodies) and the limitations of clauses related to information sharing imposed through contracts with external sources.

b. The framework needs to identify and clarify any overlaps in legislation and related legal issues and support best practices so that community organizations can be fully accountable to clients, communities, legal authorities and the public for their protection, and appropriate sharing, of private personal information.

c. The framework needs to ensure that the highest standards of privacy protection are maintained throughout organizations, that control over information is centred first with the client and secondly with the organization, and that processes of acquiring consent from clients to share information should be on an "opt in" basis. The framework needs to protect the confidentiality essential to therapeutic relationships.

Recommendations to government

9. Arms-length relationship

An arms-length relationship between ICSOs and government is the proper relationship. This relationship needs to be affirmed and supported through contractual agreements and procedural arrangements.

- Current contract language is over-broad and needs revision.
- Much of the contractual language and current procedures were developed when FIPPA was the only applicable privacy-related legislation. With the implementation of PIPA new language and procedures are required.

10. Need for a simple and shared approach to information management

There needs to be a shared and straightforward view and approach to client information and information management based on the mutual understanding that FIPPA applies to government and PIPA applies to ICSOs, including those organizations that undertake contractual work for government ministries and authorities.

- This approach needs to be incorporated across government rather than on a ministry by ministry basis.
- ICSOs must be invited to participate in the development of policy.
- Any such policy being developed by government must be shared with the community service sector prior to consultation, negotiation and adoption.

Recommendations to colleagues and to government

11. Exceptions to the General Rules

It is acknowledged the there will be exceptions to the general procedures recommended above to allow the provincial government to carry out its legitimate legal obligations such as those imposed under the *Youth Criminal Justice Act* and the *Family Child and Community Services Act*.

- There may be instances where PIPA and other statutes conflict. In these situations, there must be protocols clearly defining the treatment of the information involved, and the degree to which exceptions from PIPA are allowable must be made clear.
- In addition, it may be necessary in some rare and well-defined circumstances to have additional protocols related to
    - Transfers of personal information from the province to an external organization
    - Transfers of personal information from an external organization to the province
    - Transfers of personal information amongst several organizations where
        - Team-delivered services are offered
        - Inter-organizational case conferencing is occurring
        - Integrated case management practices are in place

Where such protocols do not adhere completely to the recommended general procedures, exceptions must be kept to a minimum, and any concerned party should be able to the Information and Privacy Commissioner for adjudication.

Appendix A: Survey of Independent Community Service Organizations

Stakeholder Survey questions

1. How many client serving programs and services do you provide in total?
2. How many of these programs and services are funded by government through grants, contributions or contracts?
3. Please provide more detail:
4. How many of your programs are multi-government funded?
5. In multi-funded programs, do the government service contracts have differing information/statistical reporting requirements?
6. In terms of managing reporting requirements on a project with conflicting reporting requirements, please choose the answer that best describes your experience in dealing with the differences:
7. Please describe generally how you deal with the conflicting requirements:
8. Has your organization conducted a privacy audit?
9. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to addressing privacy issues in your organization:
10. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to managing privacy issues of paper documents:
11. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to managing privacy issues of electronic personal information:
12. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to training staff on privacy issues and protocols:
13. Please provide any additional details and comments of interest to your answers to questions 9-12:
14. Do you have an identified privacy officer at your organization?
15. Is your privacy officer also your executive director or chief executive officer?
16. How important is confidentiality to your organization?
17. Generally, under your service contracts with government, who owns the information gathered by your programs and services?
18. Do you inform your clients that information gathered as part of the service delivered could be disclosed to government?

19. Does the disclosure of client information to government (not aggregate information for program evaluation purposes) affect the services and programs you provide?
20. Have you received any requests for disclosure of client information? (Select all that apply)
21. If you answered “yes” to question 20, what is the frequency of these requests?
22. If you answered “yes” to question 20, please describe generally how these requests are handled:
23. Generally, please select all the answers that best describe how information is gathered by front-line staff (i.e. writing up case notes, documenting visit, etc.) when working directly with clients.
24. Generally, if there is paper documentation being done with your front-line staff, how would adding an electronic client management system to the process impact how information is documented and managed?
25. Generally, if there is paper documentation being done with your front-line staff, how would adding an electronic client management system to the process impact the nature of the service and the interaction with clients?
26. Please provide any other context/comments for your answers to the previous two questions (if necessary)
27. Select the sectors that best describe the mission and services of your organizations (select all that apply):
28. Select the size that best describes your organization’s gross revenue:
29. Please select the region that best describes your service location:

Appendix B:
Survey of Independent Community Service Organizations with Results

Stakeholder Survey Results: July 15, 2008

1. How many client serving programs and services do you provide in total?
    - 720 programs and services over 36 respondents (average/organization = 20)

2. How many of these programs and services are funded by government through grants, contributions or contracts?
    - 443 programs and services reported as government funded
    - Of 36 reporting clients, only 15 (or 41.67%) had *all* their programs/services funded by government

3. Please provide more detail:
    - Of clients who broke down program funding by level of government/funder:
        i. 7.48% of reported programs were funded by federal government bodies
        ii. 64.25% of reported programs were funded by provincial government bodies
        iii. 3.74% of reported programs were funded by municipal government bodies
        iv. 10.75% of reported programs were funded by health authorities
        v. 13.79% of reported programs were funded by other funding bodies (a sample of which include: Community Living BC, United Way, and various foundations)

4. How many of your programs are multi-government funded?
    - 16 of 36 clients reported programs with multi-government funders
    - A total of 65 programs were reported as receiving funding from multiple levels of government (9.03% of the total 720 programs)

- Clients who reported programs with multi-government funding thus had an average of 4.06 programs receiving multi-government funding

5. In multi-funded programs, do the government service contracts have differing information/statistical reporting requirements?
    - 100% of respondents to this question answered yes

        - "Different funders require different information"
        - "All reporting requirements are specific to the particular funding source"
        - "Each government body has its own contract with us and therefore requires slightly different reports on slightly different templates or timelines"
        - "Federal government contract requires an onerous degree of reporting on every aspect; provincial government contract is much more flexible and appears to be collecting meaningful data through their reporting mechanisms"
        - "Different objectives so different ways to reporting activities"
        - "Different financial reporting"
        - "Each funder wants information provided in their own format and at different time intervals with differing degrees of complexity and linking to specific clients"
        - "The ministry requires different reporting than the Law Foundation for the same program"
        - "Different levels of info required, different forms"
        - "Depends on which part of the program they support, is buildings or staffing"
        - "The forms and reporting requirements are not consistent"
        - "Outcomes, measures, reporting requirements"
        - "Of course; they dictate terms of reporting without apparent regard for the extra work load this requires"
        - "Each is seeking different data and a different break down of financials"
        - "Nothing complex -- just each funder looking for their own specific bits of information. Forms are different. Time frames are different. Content is different"
        - "Age population - Youth & Adults"
        - "Pregnancy Outreach Program: extensive reporting for federal govt. & minimal reporting for IHA top-up funding"

6. In terms of managing reporting requirements on a project with conflicting reporting requirements, please choose the answer that best describes your experience in dealing with the differences:
    - 16.7% of respondents said "it is very difficult to manage"
    - 50% of respondents said "it is somewhat difficult to manage"
    - 25% of respondents said "it is somewhat easy to manage"
    - 8.3% of respondents said "it is very easy to manage"

7. Please describe generally how you deal with the conflicting requirements:
    - sampling of answers omitted in this draft

        - "Provide statistics in multi formats"
        - "We design a general format/database to capture all statistics as much as possible. We then custom-design the actual report as per each funder's specific requirements"
        - "Long term contracts have templates developed for each reporting requirement, so it is not difficult to complete it. The difficulty lies in organizing the responses to be timely due to different reporting periods"
        - "We provide stats/financial data in multiple formats that are templated to us by the contractor. At the same time, we have our own internal formats required by our accountant and by our Board members"
        - "We are providing different stats in formats that are sometimes not compatible. It depends upon the funder. We do not have common templates"
        - "I provide information in multiple formats, which is difficult and time consuming"
        - "We provide data in varying formats. No template that would work for every funder"
        - "Each program is responsible for reporting to the appropriate funder in the required format. The program annual report summarizes all funding sources. It would be impossible to have an agency template that would work for every funder. For example, some programs require SIN or PHN numbers, whereas for other programs that would be inappropriate. Some funders (MCFD) require client referenced outcomes that are not required by other funders. Demographic information varies between funders. Specialized programs require specialized reporting, for example addictions have more than 30 reporting categories (type of drug of abuse, ethnicity (that does not meet Canadian standards), previous treatment, etc. that other programs would not use. Some programs report on disabilities, other programs do not. Several of our programs are required to use government databases, but we are unable to obtain information on our clients that we need, so have to run duplicate systems. Some government ministries do their own external evaluation of programs (Multicultural services) which requires client specific information is shared. Most require internal evaluations (FHA has 8 questions that must be asked of everyone, three times: pre, during and post service; but were not client referenced. They are now requiring that new information on HONOS be submitted and be client specific). It is a management nightmare!"
        - "We have had to design very complex systems in order to capture the information to meet the reporting requirements of multiple funders"
        - "Though we have several different funders with different reporting requirements, each contract has only one funder and only one

reporting requirement. The problem is not that there are multi-funded programs; it is that we have a range of different programs and funders and that their reporting requirements are different, compounded by the fact that we are a small organization so one staff person may be providing two or more services and therefore have two or more reporting requirements"

- "It takes a lot of staff time to do reports - although we understand the need for funders to be accountable about how the funds are spent"
- "Generally the funders want different information so it is not too onerous. In cases where there are different levels, we collect for the most complicated and find the data less stringent inside that data set"
- "Agency template covers requirements of all reports"
- "Usually the funder provides the template and we hand-gather whatever is needed"
- "Designed the system well at the front end, use a database and different queries create different reports"
- "We're just starting on this program so unsure how it will turn out. In Research & Ethics, have experienced cooperation between Prov gov't, university and two school districts"
- "We respond to the required reporting"
- "Template that works for the funder"
- "Municipal-funded youth services have come up with one form, MCFD catalogue of services is useful but interpreted differently depending on the program"
- "We collect data for our agency and membership. This data is then utilized to write reports for the funder. Often we have more data available than what is required by the funder"
- "On an ad hoc (very frustrating) basis- cannot find a formula that works for everyone"
- "Currently use MIS for ministerial stats. No conflict - each program submits their own"
- "Provide data in the ways that are requested. So have to format data in two ways to deal with two different funders"
- "One of our funders has the longer, more in-depth form and we provide that to both funders. The other funder with the shorter form -- we simply do that when they require it"
- "The agency has an enterprise application that can manage very complex reporting requirements. The cost of programming is the main barrier to producing reports. Ministry changes to data requirements are costly to the agency"
- "We follow the template each funder requires. Different reports for different funders. No agency template"

8. Has your organization conducted a privacy audit?
    - 20.6% of respondents said "yes, in the past two years"
    - 14.7% of respondents said "yes, in the past five years"
    - 0% of respondents said "yes, in the past ten years"
    - 64.7% of respondents said "no, we have not"

9. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to addressing privacy issues in your organization:
    - 26.5% of respondents said “it is very adequate”
    - 29.4% of respondents said “it is somewhat adequate”
    - 29.4% of respondents said “it is somewhat inadequate”
    - 14.7% of respondents said “it is very inadequate”

10. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to managing privacy issues of paper documents:
    - 26.5% of respondents said “it is very adequate”
    - 41.2% of respondents said “it is somewhat adequate”
    - 17.6% of respondents said “it is somewhat inadequate”
    - 14.7% of respondents said “it is very inadequate”

11. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to managing privacy issues of electronic personal information:
    - 29.4% of respondents said “it is very adequate”
    - 32.4% of respondents said “it is somewhat adequate”
    - 17.6% of respondents said “it is somewhat inadequate”
    - 20.6% of respondents said “it is very inadequate”

12. Please choose the statement that best represents your view on the amount of resources your organization annually dedicates to training staff on privacy issues and protocols:
    - 17.6% of respondents said “it is very adequate”
    - 32.4% of respondents said “it is somewhat adequate”
    - 17.6% of respondents said “it is somewhat inadequate”
    - 32.4% of respondents said “it is very inadequate”

13. Please provide any additional details and comments of interest to your answers to questions 9-12:
    - sampling of answers omitted in this draft
        - “Accredited through CARF, so clear expectations exist for paper files etc. not so clear is the discussions in the hallways type of behaviour. I believe most employees and people we support know the information about them is theirs and is kept in locked cabinets with limited access”
        - “I am the privacy officer, but have reduced hours. I deal with issues as they arise. I didn't do full privacy audit before because I had a general knowledge of all of the programs and the

safeguards in place were adequate. With emerging trends though, and electronic records being instituted we have many privacy concerns, so will be conducting a privacy audit in the next two months"

- "We have very little personally identifiable information electronically or in hard copy"
- "We have a Privacy Officer who addresses all privacy issues and we have policy in place. Staff call the Privacy Officer if they have any issues/concerns. More formal training would probably result in less calls"
- "We dedicate adequate resources but we don't receive adequate resources to meet the expectations from our funders, accrediting bodies and our own professional standards"
- "What we do is very cursory in terms of security of files, papers, electronics etc.; we do a better job of disclosure; need training on requirements, and resources to put systems in place"
- "Privacy functions are considered to be assumed by the organization. Funders are not interested in funding such initiatives and assume organizations are completing privacy audits"
- "We adhere to accreditation standards, and all program directors and most staff are quite familiar with these"
- "I had difficulty in choosing between very adequate and somewhat adequate as I tend to think what we have is adequate. (My answer to 11 would be very adequate)"
- ""'Adequate'' probably misleading but no other answer fit. We do very little, are asked to do very little, provided the Privacy Officer with a manual & some time on the web site. The issue very rarely comes up"

14. Do you have an identified privacy officer at your organization?
    - 85.3% of respondents said "yes"
    - 14.7% of respondents said "no"

15. Is your privacy officer also your executive director or chief executive officer?
    - 45.5% of respondents said "yes"
    - 45.5% of respondents said "no"
    - 9.1% of respondents said "n/a"

16. How important is confidentiality to your organization?
    - 100% of respondents said "very important"
    - 0% of respondents said "somewhat important", "somewhat not important" or "not important"

17. Generally, under your service contracts with government, who owns the information gathered by your programs and services?
    - 10.3% of respondents said "the client"
    - 55.2% of respondents said "your organization"

- 34.5% of respondents said “government”

    - “Programs funded by government belong to government”
    - “MEIA funded programs ‘own’ the client file. Other gov’t funded programs the agency ‘owns’ the file”
    - “Most of our contracts are set up that the funder owns the publications we produced, but not private information gathered relating to clients”
    - “It varies according to the contract outcomes and funder requirements. generally it seems that when push comes to shove we are responsible for storing it at least”
    - “This varies depending on the ministry. Some ministries are not clear on the matter at all”
    - “We understand that the clients and government can access the info, but it belongs to the agency to keep. All three own the info.”
    - “It depends upon the service area and nature of the information. Most information is owned by either the client or the organization”
    - “Over the years we have fought for agency ownership, but subsequent contracts have eroded this. Generally, government contracts that claim ownership have never activated their request for the information, now have we been very vigilant about notifying them of destruction of documentation (which is 25 years according to agency policy, with exceptions based on contracts)”
    - “Actually, it varies, often specified in the contracts with the funder”
    - “I needed to also tick 'government' as that is the case in some contracts (MCFD)”
    - “No information is collected or passed on unless specifically authorized by the individual and/or their Agent/legal representative”
    - “The ownership varies according to which part of government we are dealing with”
    - “As per contract”
    - “Only numbers shared, no names”
    - “MCFD owns our records”
    - “Our contracts state that our agency has ownership of client files”
    - “The client and the organization also owns the information”
    - “The data gathered belongs to the contracting Ministries with the exception of the Stopping the Violence program data which belong to our agency”

18. Do you inform your clients that information gathered as part of the service delivered could be disclosed to government?
    - 96.9% of respondents said “yes”
    - 3.1% of respondents said “no”

19. Does the disclosure of client information to government (not aggregate information for program evaluation purposes) affect the services and programs you provide?
    - 51.5% of respondents said “no”
    - 48.5% of respondents said “yes”

        - “In some cases clients have expressed lack of trust due to access to their information”
        - “We think private client information should not be disclosed to government. It is our practice that we do not”
        - “Tension exists between our role as advocates and as contractors in regards to reporting accurate income or bank holdings in regards to subsidized housing reports from BCHMC”
        - “How and what we document in client files has been revised. Minimal identifying data and details of clients' history and treatment/care plans are recorded where possible”
        - “Clients would be less likely to disclose personal information to us”
        - “The majority of clients do not realize the privacy implications and just sign. Other clients are very paranoid and won't provide information. We still provide services”
        - “Some people refuse service”
        - “Some clients may choose not to participate given that information will go to funder”
        - “Clients feel less trust and sometimes hold back important information”
        - “Not really, but I needed to comment that we would opt out of providing the service should this become an issue”
        - “We only disclose information with the client’s informed consent including those covered by the criminal justice system”
        - “Young people are more suspicious of the service, less open, less trust”
        - “The majority of the client information we share relate to behaviour progress. Many of our clients are referred or select our programs through government portals and the government is aware of the client information”
        - “I believe the only time we might have to disclose client file info to government would be in the case of a child protection issue. For mothers, our requirement to report and/or our requirement to provide information may cause them to feel insecure about accessing our services and/or about telling us everything they need to/want to tell us”
        - “Affects (determines) level of Funding”

20. Have you received any requests for disclosure of client information? (Select all that apply)
    - 51.5% of respondents said “yes, by government”
    - 57.6% of respondents said “yes, by clients”

- 57.6% of respondents said “yes, by other”
- 9.1% of respondents said “no”

    - “Subpoena”
    - “Employees”
    - “Lawyers acting on behalf of a client in a legal matter have requested file information”
    - “In child custody case, client's former partner applied to have file subpoenaed. This was not successful”
    - “We have very few requests - usually from clients. Generally we have other agencies for service providers who are requesting the info.”
    - “Police, legal personnel”
    - “Mental health teams”
    - “Over the past ten years I have handled one government FIPPA request. In the past year I consulted on about 4 inquiries. Client requests are handled within programs without consulting me and agency policy allows reasonable access and photocopying. This year we had one request from a non-custodial parent in an alleged sexual abuse case with a child. I addressed his general questions and sent him the appropriate FIPPA form, but he has not proceeded. We get up to a dozen court subpoenas as well, primarily in supervised access and family support programs, and occasionally in addictions services (which included one coroners inquest)”
    - “Legal inquiries”
    - “Coroner, Police--we do not generally have the information people want because we collect none from callers”
    - “Medical, legal, other personnel”
    - “Licensing branch”
    - “Lawyers for court purposes”
    - “We have had requests from parents for access to youth files (denied) and request from non-custodial parents for the other parent's info (denied)”
    - “We have had documentation subpoenaed by police for investigations”
    - “Family court issues around custody”
    - “Courts”
    - “Other organizations that the client is connected to”
    - “Lawyers”

21. If you answered “yes” to question 20, what is the frequency of these requests?
    - 50% of respondents said “rare”
    - 36.7% of respondents said “sometimes”
    - 6.7% of respondents said “frequent”

- 6.7% of respondents said “very frequent”

22. If you answered “yes” to question 20, please describe generally how these requests are handled:
    - sampling of answers omitted in this draft
        - “We protect client confidentiality and follow the law”
        - “Requests must be accompanied by a written release from the client or a court order. Files are reviewed by the supervising Director prior to release.”
        - “The client will be asked to fill out a simple request form and provide proof of identity. We usually try to accommodate those request a.s.a.p., but we have up to 30 days to respond in our policy”
        - “In writing back and forth. if other people are mentioned we secure their approval for release”
        - “Handled by our program manager and crown counsel. Ultimately, the judge struck down both applications for disclosure, so we did not proceed”
        - “We insure that the client is aware of the request prior to sending the info.”
        - “We provide them with what they need as the request is usually accompanied by legal notification”
        - “The client must consent to the request. The request must be specific and time limited”
        - “If it is a client, agency policy is followed. If it is government, court or coroner, information is provided in accordance with the contract or law. If it is a third party, the privacy officer, program supervisor and program manager meet to discuss the concerns and how to address them”
        - “All requests are made in writing and the program supervisor and privacy officer are both informed”
        - “We have 30 days to respond. I (ED/PO) review the file and indicate what should be copied and what should not or needs to be edited to eliminate confidential information about 3rd parties”
        - “Clients see their files through program staff. Government received all files at program termination, boxed and labeled. Historical information must first be retrieved from off site secured storage”
        - “Goes to ED, responded to based on context of request”
        - “If it is by government, it is outlined in the contract and clients understand this ahead of time in terms of what sort of information may be disclosed and reports written etc. Clients are always given a copy of any report. If client has requested a copy of their own file, they must fill out a PIPA Request to Access Personal Information form”
        - “Unless authorized by the individual/Agent/representative we decline to release such information”
        - “We follow a 30 process and have clearly defined policy etc. inclusive of training for staff”

- "Request is reviewed by the ED and responded to accordingly"
- "Written request to the Privacy Officer"
- "Request is denied, person served is advised of the request"
- "With legal advice"
- "There is a process that the privacy officer"
- "If from client, through release of information request. If through abuser, we involve our counsel"
- "On an individual basis"
- "Government can subpoena client files. We provide these for court - but only reports generated by our agency, not third party reports. Clients specify who we can release information to. We only release information generated by our agency. Clients fill out a specific consent every time information is shared"
- "Unless we have signed consent from the client we don't provide the information. We often have to go and get consent"
- "When clients want to see their files, we are happy to allow this. When we get requests for our files from others our usual response is to contact our lawyer who then takes the matter in hand, seeks resolution (no sharing of files), and if we are still required (order by judge), then we provide the file"
- "All information is reviewed my manager then reviewed again by the privacy officer"
- "Quarterly reports"
- "Regarding gov't requests for info, I am referring to monthly AIMS forms reporting which requires disclosure of clients' full names and addictions-related info. Otherwise there is only the occasional client request for info. If we are satisfied there is no 3rd party info in the file, we generally give the client the info they ask for. We are NOT trained in procedures for releasing client info, however"

23. Generally, please select all the answers that best describe how information is gathered by front-line staff (i.e. writing up case notes, documenting visit, etc.) when working directly with clients.
    - 81.3% of respondents said "it is done on paper in front of clients"
    - 43.8% of respondents said "it is done on paper, but only after the client visit is over"
    - 43.8% of respondents said "it is done on paper and re-entered electronically afterwards"
    - 28.1% of respondents said "It is done electronically with front-line staff inputting answers into a computer or handheld device directly as they are interacting with clients"
    - 15.6% of respondents said "other"

        - "Personal goal plans stats are done by collating reported outcomes, sometimes with the person present, sometimes without. It is quite individual"
        - "Usually talk over the phone, info written down on paper"
        - "Phone only service-call stats entered after calls"

- "Also done in front of clients. Typically notes are made and then entered into our database, which is developed by National and consistent among agencies"
- "Done electronically after the client visit"
- "We are required to submit (in electronic format in some cases) our statistics, so some client information gets entered electronically and uploaded to funders -- but this is quantitative data, much less likely to be directly identifiable"
- "Moving to all data collected electronically"
- "There are times when paperwork must be done in front of the client in order to capture information"

24. Generally, if there is paper documentation being done with your front-line staff, how would adding an electronic client management system to the process impact how information is documented and managed?
    - 63% of respondents said "it would have a positive impact"
    - 18.5% of respondents said "it would have no impact"
    - 18.5% of respondents said "it would have a negative impact"

        - "Contained in a central location with added security. Additional format and back-up"
        - "We already have both a paper and electronic system- the former for the detail of visits etc. and the electronic to track statistical information"
        - "The electronic portion of the client information is mainly for statistics reporting. The paper document contains more private client information than our databases"
        - "We have purchased sharevision and will be hiring a coordinator to implement the client info management system. we believe it will go a long way to increasing appropriate access by the people we serve to information about themselves. may also increase efficiency for government reporting"
        - "First off, we would need fewer filing cabinets and file storage space. Information would potentially be more secure than our paper files. The recording would be more efficient and much less use of paper, pens, and other stationery supplies"
        - "This would be temporary until everyone got used to it" (re. negative effect)
        - "But it very much depends on the complexity of the system, staff experience with electronic records. Some staff are afraid and resistant, most try to learn. Our main concern is how to verify that information is accurate, reliable and unbiased and protected from unauthorized disclosure or accidental deletion for both paper or electronic records"
        - "We have begun researching various systems to use in our organization. We will likely need to use more than one system because we are a multiservice organization and the data we collect and track is different across program areas"

- "It would add to the work-load of the staff and reduce the number of clients we are able to serve"
- "We are in the process of moving from paper to electronic in order to create efficiencies"
- "Not sure how to answer -- as it would depend on the flexibility and information gathering relevancy of the management system"
- "It is what we do now-national HOMES database"
- "More work for worker and agency re security"
- "It would note when consents need to be signed again"
- "Once information is in the "system" it cannot be clarified"
- "Staff in general do not trust electronic data storage as being secure. There would have to be some education of the system being used"
- "We have an electronic client information system. Most reports are on the electronic system. There still is a paper file, with some reports and some signed documents"
- "I think this is the direction we need to move in -- but we don't know much about it, and some staff are much less comfortable with computers than others -- so while I think it will probably be a good thing, it will not necessarily be a smooth thing"
- "The electronic database the agency uses saves time. Moving the agency to all electronic recording would also mean all lists would be consistent (and annual stats would all report the same information)"
- "We do not have an electronic client management system, impression is that it would not be a concern"
- "Not sure"
- "It forces continuity and organization in file-keeping"

25. Generally, if there is paper documentation being done with your front-line staff, how would adding an electronic client management system to the process impact the nature of the service and the interaction with clients?
    - 37% of respondents said "it would have a positive impact"
    - 37% of respondents said "it would have no impact"
    - 25.9% of respondents said "it would have a negative impact"

        - "Information is appropriately shared with only relevant workers"
        - "We see people sitting together and in some cases the person we support manipulating the information"
        - "Efficiencies of time would be passed along to allow additional client time. Clients may feel more confident that information about them is recorded on a secure site (reverse could also be true - they may feel more threatened)"
        - "This would also be temporary, but more efficient in the long term" (re. negative effect)
        - "It would vary depending on the program, staff member and client. We are finding with our youth clients that electronic access through social networking is very useful, but are very concerned about privacy and the appropriateness of services in this manner"

- "I think clients would be wary of providing information"
- "I think it would save time and therefore allow more time for the actual services vs. information collecting"
- "We wouldn't do if it had a negative impact -- would depend on flexibility of system"
- "Clients with mental health issues who have been oppressed by the system do not trust information that they cannot see nor know how it is controlled"
- "May increase suspicion of who sees the data and where does it go"
- "The only potential challenge is printing off the information to review with the client when applicable. If the system was capable of this task it would not be a concern"
- "Our services are built on trust. This would not engender trust"
- "I hope it would have no impact"
- "It does seem to have a negative impact now (about 1 year into the process) as some duplication is seen. The processes need to be pared down so that there is no duplication between paper and electronic input"
- "I'm not sure -- perhaps it would save time over the long run, which might allow for additional client sessions? In one of our programs, staff fill paperwork out while sitting with the client -- so moving to doing that on computer might increase our clients' fears about where the information "was going" -- which might increase time spent with each client on intake"
- "The programs that have moved to all electronic reporting are encouraging other programs to move over due to the enhancements they are gaining"
- "Not sure"
- "There needs to be a selection for "it depends." Some of our current systems are excellent and user-friendly. Others are impossible and time-consuming to use. A system should be useful to front-line staff, not just gov't collectors of data"

26. Please provide any other context/comments for your answers to the previous two questions (if necessary)
    - sampling of answers omitted in this draft

- "We use an electronic client management system"
- "Again it varies significantly between each program, depending on the people served and the intent of the service"
- "The question about electronic client management immediately begs the question of who owns this data, storage of this data, etc."
- "Any system should have a benefit to the staff and agency and it should be very easy to access and input"
- "If information system could capture and provide meaningful data analysis then it could be very useful and could have a very positive impact. The cost benefit would then be in how the

information is collected and inputted without impacting on the individual's lifestyle"

- "Security of an electronic client management system must be highly defined. Who will be managing protected information to ensure it cannot be hacked into, reviewed by non-trustworthy sources and be separate from review of other organizations"
- "Our file review process for Continuous Quality Improvement needs to be refined. Historically we had a team of people that went to each program to review random paper files. This can be done now from one site as client info system is web-based. We need to look at which paper files still need to be reviewed, and whether paper and electronic systems can be better merged to avoid duplicating work"
- "(I am responsible for the database system) The agency is committed to moving to 100% electronic reporting"
- "As a non-profit organization, we do not want to be recognized as a government organization, I think it is vital to connect directly first and gather the information in a non-bureaucratic manner"
- "Would depend on cost, capability, and flexibility of electronic management system"

27. Select the sectors that best describe the mission and services of your organizations (select all that apply):
    - 59.4% "Children and youth services/housing"
    - 53.1% "Services for the physically or mentally challenged"
    - 46.9% "Family and crisis counselling, financial counseling"
    - 37.5% "Housing for seniors, low income & those with disabilities"
    - 37.5% "Other services for low-income people"
    - 34.4% "Employment preparation and training"
    - 34.4% "Emergency shelter"
    - 34.4% "Addiction services and support groups"
    - 28.1% "Mental health services and support groups"
    - 25% "Services for aboriginal people"
    - 21.9% "Legal assistance and services"
    - 21.9% "Crime prevention, public safety, preservation of law & order"
    - 21.9% "Training, education"
    - 15.6% "Food or clothing banks, soup kitchens, hostels"
    - 15.6% "Seniors' services"
    - 15.6% "Public education, other study programs"
    - 15.6% "Research (scientific, medical, environmental, etc.)
    - 12.5% "Rehabilitation of offenders"
    - 12.5% "Promotion and protection of health"
    - 9.4% "Day care/after-school care"
    - 9.4% "Human rights"
    - 6.3% "Cultural programs, including heritage languages"
    - 6.3% "Youth groups (Girl Guides, cadets, 4-H clubs, etc.)
    - 6.3% "General environmental protection, recycling services"

- 6.3% “Support and services for the charitable sector”
- 3.1% “Scholarships, bursaries awards”
- 3.1% “Vocational and technical training”
- 3.1% “Festivals, performing groups, musical ensembles”
- 3.1% “Cultural centres and associations”
- 3.1% “Other mutual support groups (e.g., cancer patients)”
- 3.1% “Community recreation facilities, trails, etc.”
- 0% “Specialized health organizations”, “Nature, habitat conservation groups”, or “Preservation of species, wildlife conservation”

28. Select the size that best describes your organization’s gross revenue:
    - 0% of respondents said “< $98,000”
    - 0% of respondents said “$98,001 to $256, 000”
    - 25% of respondents said “$256,001 to $750,000”
    - 12.5% of respondents said “$750,001 to $1,275,000”
    - 34.4% of respondents said “$1,275,001 to $5,451,000”
    - 18.8% of respondents said “$5,451,001 to $12,049,000”
    - 9.4% of respondents said “>$12,049,001”

29. Please select the region that best describes your service location:
    - 59.4% of respondents said “Lower Mainland”
    - 15.6% of respondents said “Thompson-Okanagan”
    - 9.4% of respondents said “Province-wide”
    - 6.3% of respondents said “Vancouver Island”
    - 6.3% of respondents said “Kootenay”
    - 3.1% of respondents said “North”

Appendix C:
Melissa's Story[65]

Case Study Number 1 – PLEA Community Services Society

PLEA Community Services Society *operates in the Vancouver area. Through unique services tailored to individual strengths and needs, PLEA helps children, youth, adults and families with significant challenges to lead fulfilling lives within their communities. PLEA delivers youth justice, youth addictions and other support programs; the KidStart Mentoring Program; and specialized residential services for youth and adults with a range of social and health needs.*

Most of the programs operated by PLEA have been operating in some form since 1973 – and many arose from within the community they serve. In 1984 with the privatization of community based youth services, PLEA became an incorporated not for profit society with an independent Board of Directors. Though they receive funding from various Ministries, they also receive funds from municipal government, Health Authorities, the United Way and other private funders. Their mission, programs and services have a completely separate legal existence from their funders.

Each visit or contact is logged manually after each visit. Contact logs may reflect the emotional state of the youth as well as their concerns and hopes for the day and the future. For Detox, contact logs are kept in paper copy. Client demographic, presenting issues and discharge information are included on CAMS. Whether she stays for 1 day or 10 all her records are retained. Over the course of each contact with PLEA Lisa may have contact with Melissa several times in the course of a week, as well as multiple contacts with other workers involved with her service plan. At the end of the day, Lisa enters information into CAMS. She is authorized only to enter information in the Detox program, and while she can review information provided at Melissa's previous intakes, she is unable to access the notes of Melissa's involvement in other PLEA programs.

Before any case notes are posted onto CAMS, a supervisor will have approved their content. Only individuals with specific access are authorized to access the information at any given stage on CAMS. As with all records at PLEA, every effort is made to keep the records as factual as possible, and free of opinion, judgment or speculation. However, notes may still contain some information about third parties.

[65] *Melissa's Story* is a composite case study created for illustrative purposes as part of the research process. These stories are informed by the information gathered at the four site visits and are therefore based on the realities currently faced by ICSOs, but are composite stories so as to not be identifiable as any actual client.

All staff are aware of section 110 of the Youth Criminal Justice Act and its prohibition on disclosing information related to a youth in conflict with the law. This further reinforces the high premium placed on privacy and confidentiality by workers at PLEA as they provide services to clients.

In order for Melissa to succeed she needs help. PLEA keeps an archive of her life and struggles over many years. In many cases, PLEA is the custodian of much of a youth's life story until the point at which they cease contact. All of the information they collect is related to the provision of programs and services to their clients.

For **Melissa**, PLEA is a lifeline. Between her first visit in 2005 and the present day (2008), Melissa has accessed PLEA services 24 times, including multiple stays in Detox, the Supported Recovery program, and ONYX Vancouver. She has come to see Lisa, an intake worker with PLEA, to access a Detox program after having previously completed the Daughters & Sisters program. She says she suffers from a learning disability, and has been diagnosed with Hepatitis C. She sometimes lives with a boyfriend who is also an addict. She describes herself as Métis and Christian. She gives Lisa her Care Card Number but does not have a SIN number. Her picture is taken for inclusion with her file.

Lisa works with the Detox and Supported Recovery programs of PLEA. She has a BA in criminology. In her 8 years at PLEA, she has taken professional development courses in suicide intervention, crisis intervention training and conflict resolution. Lisa needs to develop an immediate relationship of trust with Melissa to help her move through her situation. She meets with Melissa at the home where she will detox from her drug of choice, crack cocaine. She takes no notes during the meeting though she brings a notebook with contact log sheets and various information packages to leave with Melissa.

At the meeting, Lisa gives a Melissa the Release of Information form and a pamphlet with more information about her privacy rights. Records of Melissa's stay, including both her emotional and physical state throughout are maintained in contact logs held in binders at the caregiver's home. When she leaves the caregiver's home, the records will be sent to PLEA's office in Surrey.

Unlike the Detox program she is currently accessing, in Daughters & Sisters (where Melissa has previously been treated), PLEA is contractually required to report to the referring agents (Probation Officers [PO]). For Daughters & Sisters, all information is available on CAMS (contact logs, reports, assessments). Only authorized users can access information on CAMS, and then only within the circle of care of the client. The circle of care is a term used to describe the network of staff, resources and services specifically directed to providing care for each client of PLEA. While a client is at Daughters & Sisters, the assessments and reports created on CAMS are shared with their PO, however the POs do not have access to client information on CAMS themselves.

At their next meeting, Melissa and Lisa discuss confidentiality. Lisa is very concerned about potential disclosures to her boyfriend. Lisa reassures Melissa, because in her view, the strong commitment to confidentiality is key to the success of the programs of PLEA. The Release of Information form is completed at each intake Melissa has with PLEA.

Appendix D:
Sam's Story[66]

Case Study Number 2 – Abbotsford Community Services Society

Abbotsford Community Services (ACS) *is a non-profit, multi-service, community based agency providing services in Abbotsford and surrounding communities in the Fraser Valley since 1969. ACS has 70 programs operating throughout the Fraser Valley and work in a complex contractual circumstance with multiple funders from various levels of government.* ACS puts a high premium on confidentiality throughout the addictions program. In order to ensure confidentiality Jerry and the care team also have had training on "need to know" and its application at all levels of their services. The self-assessments, and his case notes remain entirely within the confines of the program. Aggregate data to the funders.

ACS has 70 programs operating throughout the Fraser Valley. They do not combine files from different programs for the same individual, so Sam may have six (or more) different files held by the program where he's accessing the particular service. There is no place at ACS where someone could go and find out where Sam has files.

ACS puts a high premium on confidentiality throughout the addictions program. In order to ensure confidentiality Jerry and the care team also have had training on "need to know" and its application at all levels of their services. The self-assessments, and his case notes remain entirely within the confines of the program. Aggregate data to the funders.

ACS has 70 programs operating throughout the Fraser Valley. They do not combine files from different programs for the same individual, so Sam may have six (or more) different files held by the program where he's accessing the particular service. There is no place at ACS where someone could go and find out where Sam has files.

Sam, 42, has a drug problem. He has bi-polar disorder for which he is on medication. Sam has had a difficult time. He or members of his family have been clients of Abbotsford Community Services (ACS) for many years. He relies on all the members of

[66] *Sam's Story* is a composite case study created for illustrative purposes as part of the research process. These stories are informed by the information gathered at the four site visits and are therefore based on the realities currently faced by ICSOs, but are composite stories so as to not be identifiable as any actual client.

his care team to ensure that the information he provides is kept confidential. This trust is core to the culture of Abbotsford: “People have the right to be forgotten or forgiven. . . . How do I know that this information isn’t going to be misused in the future?”

Sam is an MCFD “mandated” referral by a protection team. After the referral, Sam attends a group orientation at ACS. While there, Sam fills out an orientation form. Sam has a week to call back and when he does an addictions counselor is assigned. Had he not called back all the initial information collected would have been destroyed.

Jerry is Sam’s addictions counselor. He has a Master’s degree in counseling psychology and 10 years of experience. At their first meeting, Jerry asks Sam to tell him about himself and to assess his priority needs. Jerry gives Sam a Clients’ Rights brochure. Sam also fills out a Michigan Alcohol Screening Test (MAST), and the Drug Abuse Screening Test (DAST),

Jerry and the care team developed a Client Service plan that Sam signed along with a Confidentiality Agreement and a Confidential Self-Assessment. He is given a copy of the plan. The plan also includes accessing a range of services including the food bank, a parenting class, and potentially residential treatment. While in the program, Sam will be asked to sign a consent or release form.

Sam’s son Philip is in foster care right now. Sam wants to maintain the relationship, so he also comes to ACS for supervised visits with Philip. Darcy is the supervised access worker. She has a certificate in social services and has been working for the agency for 5 years. She records verbatim notes of the visits between Philip and Sam. Her report then goes to clerical for typing and is sent back to be read and verified. All reports read by supervisor are sent to the MCFD assigned social worker. The paper file is held on site for 2 years, and then boxed, labeled, and sent to Iron Mountain for storage.

Client Confidentiality Form used by Abbotsford Community Services

Most Client Information gathered by Abbotsford Community Services is strictly confidential. There are, however, some limits to confidentiality. Under these limits information will be shared with the appropriate authorities. These limits include:

1. child abuse or neglect;
2. danger to physical safety of a person (threats, suicidal, driving while intoxicated);
3. court order for the release of records or testimony;
4. discussion of counsellors' casework during supervision in their programs;
5. Workers' Compensation Board investigation of a compensation claim;
6. requests through Freedom of Information Act applications;
7. program quality surveys; and
8. information required by our funders.

Any other information regarding your involvement with ACS services will only be with your written consent. Consent expires one year after this consent is signed. Consent can be withdrawn in writing at any time. After the date of receipt of your written withdrawal of consent no further information will be released unless required in 1 to 8 above.

- I have read and understand the limits of confidentiality. Yes No
- I have been given a copy of my rights and responsibilities. Yes No
- I consent to participate in this ACS Program. Yes No

_____ _____ _____
Client Name Client Signature Date

_____ _____ _____
Witness Signature Copy Taken/Declined Expiry Date

This consent expires one year from the date of signing.

Appendix E: Bobby's Story[67]

Case Study Number 3 – Victoria Women's Transition House (VWTH)

Victoria Women's Transition House (VWTH) *– Since 1975, several thousand women have come to the doors of Victoria Women's Transition House looking for help, seeking a brighter future for themselves and their children. VWTH provides a safe, welcoming shelter, respectful counselling, support and advocacy. Their purpose is to, "provide a helping hand and a safe place for women to envision a new future."*

The Victoria Women's Transition House Society has been working to provide emergency and second-stage transition housing to women and their children fleeing domestic violence since 1975. Currently, they operated an emergency shelter, second-stage housing, victim accompaniment, and individual and group counselling to women as well as the Children Who Witness Violence (CWWV) program. The CWWV program provides group counselling and one on one counselling to children depending on their age and geographic location. All referrals to the program come from the child's mother.

VWTH follows the records keeping guidelines established by the BC & Yukon Transition Society. To ensure the safety of women and children fleeing domestic violence all records are destroyed after 7 years. The files are kept on site for two years and destroyed after seven. The Society does not maintain a centralized filing system containing all the records. Appropriately for files of such high privacy sensitivity, many safeguards are used to ensure file security. There are security cameras at each site operated by the Society. All filing cabinets are kept under lock and key. There is/is not a master key. All doors are locked when offices are not in use. Records of building entries are kept at all reception desks.

Most counseling records are maintained manually. What electronic records there are, are maintained by a designated staff person. E-mails from one worker to another are encrypted. There is an intranet that has firewalls and is password protected. The Society does not use a public internet service provider. They use digital signatures to further protect the information that may be sent electronically. They are currently contemplating

[67] *Bobby's Story* is a composite case study created for illustrative purposes as part of the research process. These stories are informed by the information gathered at the four site visits and are therefore based on the realities currently faced by ICSOs, but are composite stories so as to not be identifiable as any actual client.

updating their systems. Electronic reporting to the relevant Ministries is provided in the aggregate. There is no disclosure of identifiable personal information outside the Society.

Bobby, age 11, started seeing Jane his group CWWV counselor in March and started participating in April in Group B after school on Wednesdays. He has been having trouble in school, and his mother Pam has referred him to the program. Pam separated from her husband for two years because of his frequent violent outbursts. Pam, Bobby and Caroline, age 6, spent 30 days at Lucy's House, a transition house, and with the help of the staff of the society, found an apartment. Pam has been to Provincial Court and now has sole custody of her children. Her ex-husband has limited access. There are ongoing access-related issues that are being worked on through the Family Justice Program of the Ministry of Attorney General. Since Pam left, there has been no violence towards the children. All the information related to the family is kept on Pam's file, which is maintained by the counselling program staff.

Every time Bobby attends CWWV, he draws a picture that reflects his feelings on that day. Jane keeps progress notes about Bobby at each appointment. The notes keep track of the focus of the session, strategies used, Bobby's affect and remarks. During one meeting, Bobby tells Jane that he has been feeling very anxious and describes some interactions he has had with kids at school. Jane records what Bobby has said by putting his comments in quotation marks. On one occasion Pam tells Jane that she fears Bobby is depressed and asks Jane to follow up with a doctor at 222-1111. Her notes also reflect whatever follow-up she has recommended. Jane keeps the file manually for practical reasons. She has been a counselor with the society for 20 years. She has a BA and many professional development and external counselling certificates from postsecondary institutions. For the past five years, she has worked exclusively with the CWWV program. From her point of view working with children requires a high level of interaction – it would be impractical to keep such records electronically.