OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

INVESTIGATION REPORT F10-01

MINISTRY OF HOUSING AND SOCIAL DEVELOPMENT
MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT

Paul D.K. Fraser, Q.C.
A/Information and Privacy Commissioner

February 8, 2010

Quicklaw Cite: [2010] B.C.I.P.C.D. No. 3
CanLII Cite: 2010 BCIPC 3
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-01.pdf

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] On April 7, 2009, an employee of the Ministry of Children and Family Development ("MCFD") was arrested by the Royal Canadian Mounted Police ("RCMP") on suspicion of fraudulently obtaining identification. During the course of the search of the employee's home that followed the arrest, RCMP officers discovered that the employee had over 400 pages of government documents containing sensitive personal information in his possession. The personal information was about more than 1400 clients of the Ministry of Housing and Social Development ("MHSD") and MCFD. The RCMP discovery set off investigations by the two ministries that resulted in the termination of the employee. Approximately seven months after the employee's arrest, the affected clients received letters from MHSD and MCFD ministries notifying them of potential harm and advising them to take precautions.

[2] These events have resulted in considerable concern in the public and within the government about the vulnerability of sensitive personal information contained in government documents.

[3] On October 21, 2009, the Minister of Citizens' Services requested that the Government Chief Information Officer ("GCIO") undertake an internal review. The BC Public Service Agency ("BCPSA") was requested to examine the human resource policies and practices related to the privacy breach. This review was conducted by the Ministry of Public Safety and Solicitor General. On October 22, 2009, the GCIO informed the Office of Information and Privacy Commissioner ("OIPC") of the privacy breach. The OIPC announced shortly afterwards that it would conduct an independent investigation.

[4] The GCIO and the Ministry of Public Safety and Solicitor General on behalf of the BCPSA published reports on January 29, 2010, containing findings and recommendations that expressed general agreement on next steps.

[5] Upon my appointment as Acting Information and Privacy Commissioner on January 25, 2010, I decided that the public interest would best be served if this report included comments on the findings and recommendations already published. The release of this report has, therefore, been delayed for 10 days. The focus of this report is to identify solutions that will assist government ministries and other public bodies to fulfill their legal obligations under the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

[6] This report results from the OIPC's investigation into the government's response to the police discovery of sensitive personal information. The focus of this report is to identify solutions that will assist government ministries and other public bodies to fulfill their legal obligations under the FIPPA.

[7] This investigation was conducted under the authority of s. 42(1)(a) of FIPPA:

> **General powers of commissioner**
>
> 42(1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations and audits to ensure compliance with any provision of this Act,
>
> …

2.0 INVESTIGATION PROCESS

[8] Investigators from the OIPC observed and participated in interviews with many of the individuals from various ministries who were involved in this matter. The GCIO organized most of these interviews. The OIPC also reviewed a collection of incident summaries, briefing notes, investigation reports, timelines and emails. Finally, OIPC investigators reviewed government policies, procedures, policy summaries and guidelines.

3.0 BACKGROUND

[9] I have reviewed the GCIO's *Internal Review*[1] and the BCPSA's *Privacy Breach – Human Resources Review*.[2] I agree with the chronologies of events presented in both reports and rather than repeat them I have summarized below the key events.

[10] In October 2006, the Ministry of Employment and Income Assistance (now MHSD) hired the employee as an auxiliary Employment Assistance Worker ("EAW"). The employee remained in this position until MCFD hired him in September 2007, as a medical benefits supervisor in the Children and Youth with Special Needs Program. Of relevance to this investigation is that during 2008 the employee was involved in assessing the eligibility of individuals who were applying for a government sponsored smoking cessation program. In particular, the employee was contacting applicants to advise them of their eligibility.

[11] On April 7, 2009, after liaising with security officers of the Government Security Office ("GSO security officers"), the RCMP attended MCFD offices in

---

[1] *Internal Review – Privacy Breach, Ministries of Housing and Social Development & Children and Family Development*, Office of the Chief Information Officer, January 29, 2010. http://www.gov.bc.ca/citz/down/privacy_breach_hr_review_jan_29_2010.pdf.

[2] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*, Ministry of Public Safety and Solicitor General, January 29, 2010, http://www.gov.bc.ca/citz/down/gcio_internal_review_report_hsd_mcfd_breach_jan_29_2010.pdf.

Victoria and arrested the employee on a matter unrelated to his employment. MCFD revoked the employee's systems access and initially instructed him to stay away from the workplace.

[12] Subsequent to the arrest, the RCMP searched the employee's home. The RCMP found two envelopes of government documents ("documents"). They were later determined to belong to MCFD and MHSD. The RCMP also seized a number of computers and equipment that could be used to create false identification.

[13] One envelope contained eight Caseload Management Reports ("caseload reports"). Caseload reports were routinely assigned to each EAW monthly. The discovered caseload reports were dated from December 2006 to April 2007. They contained file summaries of over 1400 MHSD clients, including personal information such as names, birth dates, addresses, Social Insurance Numbers ("SINs"), Personal Health Numbers ("PHNs") and benefit amounts.

[14] The second envelope contained screen printouts ("screen prints") from MCFD's data system, the Management Information System ("MIS"). The screen prints contained the personal information of 21 individuals. In the case of 17 of these individuals, the screen prints disclosed their names, birth dates, SINs and PHNs. The printouts included print dates ranging from March 2008 until September 2008.

[15] On April 9, 2009, the RCMP provided the GSO security officers with a copy of a page from a caseload report and the GSO security officers took the copy to MCFD to determine whether the employee was authorized to have the documents at home. The employee's manager confirmed that the employee was required to have access to the information and that the manager had given the employee permission to take files home to carry out certain job duties. The GSO security officer concluded that the RCMP had not discovered a "loss" or "security breach".

[16] In reaction to the arrest, MCFD conducted an internal review of the employee's system access and email use. The Senior Director in the employee's branch contacted the RCMP to determine whether its investigation should be of concern to MCFD. The RCMP told the Senior Director that its investigation was related to the employee having identification under two names but did not disclose details about what had been found in the home or disclose that the employee had previous criminal convictions.

[17] The employee returned to work on April 27, 2009 and his systems access was restored. The employee's manager was directed to oversee the employee's system access and implement a method of tracking the employee's

daily activities. This supervision ended after approximately one month. Following a May 20, 2009, interview with the employee, MCFD concluded there was insufficient evidence to pursue further action against the employee.

[18] On July 14, 2009, the RCMP met with MCFD's Information Security Officer ("MCFD ISO") and returned the documents. The RCMP also indicated that no charges had been laid against the employee and that the employee was previously convicted in BC for counterfeiting related offences.

[19] On July 15, 2009, the Director of MCFD Strategic Human Resources ("MCFD Strategic HR") informed the MCFD ISO that the caseload reports in the large envelope appeared to belong to MHSD and the screen prints appeared to belong to MCFD.

[20] On July 20, 2009, the MCFD ISO met with the Senior Advisor and Senior Privacy Analyst for MHSD ("MHSD Privacy Officers") to review the large envelope of caseload reports and provide background information about the employee. Based on its review of the caseload reports, the MHSD Privacy Officers determined that a privacy breach had occurred. Later that day, the MHSD Privacy Officers informed the Executive Director of MHSD Strategic Human Resources ("MHSD Strategic HR") of the privacy breach. The MHSD Privacy Officers advised both the MCFD ISO and the MHSD Strategic HR that this was a privacy breach and it should be reported to the Information and Privacy Commissioner. The privacy breach was not reported to the OIPC until October 22, 2009.

[21] On July 22, 2009, the MCFD ISO handed the caseload reports over to the MHSD Strategic HR.

[22] On July 27, 2009, the MCFD ISO met with the employee's manager and a representative from MCFD Strategic HR to review the screen prints. According to the MCFD ISO, the employee's manager indicated that the screen prints were MHSD documents. A day later the employee's manager confirmed that the employee was authorized to access the screen prints for his work and that he was authorized to take them home.

[23] On July 31, 2009, an investigator at the Property Loss Management Services Branch, MHSD ("PLMS investigator") received the documents and began an internal investigation to determine to whom the documents belonged and whether information in the documents had been used for criminal purposes.

[24] On October 15, 2009, the PLMS investigator concluded that, while the employee was authorized to have access to the caseload reports when employed by MHSD, he was not authorized to take them home. The investigator reported to MCFD that the employee had exploited a weakness in the criminal record check process. MCFD immediately suspended the employee, revoked his

system access and revoked his access to the workplace. MCFD dismissed the employee on October 22, 2009.

[25] On November 13, 2009, the MHSD Regional Office mailed its notification letters.

[26] On November 16, 2009, MCFD mailed its notification letters.

[27] On November 19, 2009, after discovering that the names and addresses of affected individuals were not correctly matched, the MHSD mailed another set of notification letters.

4.0 DISCUSSION

[28] Public bodies in British Columbia are statutorily required to take reasonable measures to protect personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[29] Where a breach of privacy occurs, the public body must take prompt action to ensure that the breach is contained and where appropriate to prevent similar occurrences. In order to help public bodies evaluate their compliance with the FIPPA security standard, the OIPC has published four key steps for managing a privacy breach.[3] When a privacy breach occurs, public bodies and service providers need to make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. The OIPC has applied this standard in our review and evaluation of the Ministries' actions in response to the privacy breach under investigation.

[30] **4.1 Issues**—This report examines two issues:

1. At the time the breach occurred did MHSD and MCFD have reasonable security measures in place to protect the personal information as required by s. 30 of FIPPA?

2. Did MHSD and MCFD take reasonable steps in responding to the privacy breach?

[3] The OIPC has produced a document entitled, "Key Steps in Responding to Privacy Breaches" available at: http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf.

[31] **4.2 Were the Security Arrangements Reasonable?—**At the time the breach occurred did MHSD and MCFD have reasonable security measures in place to protect the personal information as required by s. 30 of FIPPA?

[32] Former Commissioner Loukidelis noted, in Investigation Report F06-01[4] that the sensitivity of the personal information may be a factor in determining what level of security is "reasonable":

> The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.

Analysis of MHSD security arrangements

[33] During the period the employee worked as an auxiliary EAW, the MHSD Regional Office in Victoria produced and distributed the caseload reports to EAWs on a monthly basis. According to MHSD, EAWs were required to keep the caseload reports locked up after hours and, when the caseload reports were no longer needed, EAWs were required to turn the report over to administration staff for disposal. MHSD supervisors told EAWs not to remove the caseload reports from the office.

[34] While MHSD communicated to its employees what was required to protect the privacy of the caseload reports, it did not implement a records management process that would allow it to confirm that staff had securely disposed of the caseload reports. Unauthorized access to or disclosure of caseload reports could create a very high risk of financial harm to the affected individuals. Given that the caseload reports contained highly sensitive personal information, the security arrangements should have had a proportionate degree of rigour. Appropriate security arrangements would have included a method to verify the secure disposal of all caseload reports. In this case, the employee was able to remove caseload reports from the workplace and take them home where they appear to have been stored for approximately two years. The loss of these reports remained undetected by MHSD for the entire period.

[35] I find that MHSD did not make reasonable security arrangements, as required by s. 30 of FIPPA, to protect the personal information in the caseload reports. As a result, client personal information was subject to unauthorized access.

---

[4] [2006] B.C.I.P.C.D. No. 7, Sale Of Provincial Government Computer Tapes Containing Personal Information, March 31, 2006.

[36] As noted earlier, MHSD stopped creating and distributing caseload reports in the spring of 2007.

Analysis of MCFD security arrangements

[37] As noted earlier, the MCFD manager responsible for the employee confirmed that the employee was authorized to work at home and to take the screen prints home for that purpose. In my view, two "reasonable security" issues need to be examined.

[38] A public body may disclose personal information to an employee in accordance with s. 33.2(c) of FIPPA which provides:

> 33.2 A public body may disclose personal information referred to in section 33 inside Canada as follows: …
>
> (c) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the office or employee or minister;

[39] Therefore, employees are only permitted to access personal information necessary for the performance of their duties. In this case, I have concluded that the employee took home more personal information than was necessary to complete his work. Based on MCFD's explanation of the employee's role in the smoking cessation program, the employee was calling program applicants to do two things. The employee called applicants to determine if they still wanted to join the smoking cessation program. If so, and if the applicant was a current client of MHSD on income assistance, the employee was to tell them they would be receiving the smoking cessation package from MHSD. According to MCFD, the critical piece of information that the employee needed was whether the applicant had an open client file with MHSD. He did not require birth dates, PHNs and SINs to do this. Reasonable security arrangements in these circumstances required the employee to remove any personal information from the screen prints that he did not need before transporting the documents out of the workplace.

[40] The second issue here is the unauthorized access to client information. The RCMP discovered the screen prints on April 7, 2009. Apparently, the documents remained in the employee's home approximately six to 10 months after he took them home. MCFD stated that it did not know, and had no method of determining, what personal information the employee had at home at any one time.

[41] Security arrangements employed to protect this type of personal information required a level of rigour proportional to the sensitivity of the information. In these circumstances, MCFD should not have authorized the removal of government documents containing sensitive personal information

without confirmation that the employee was providing reasonable security and ensuring that the records were returned to the ministry immediately after use.

[42] I find that MCFD did not make reasonable security arrangements, as required by s. 30 of FIPPA, to protect client personal information contained in the screen prints. As a result, client personal information was subject to unauthorized access.

[43] **4.3 Did the Ministries Take Reasonable Steps to Respond to the Privacy Breaches?**

What is a privacy breach?

[44] A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information that is in the custody of or under the control of a public body. Such activity is "unauthorized" if it occurs contrary to the provisions of FIPPA.

[45] In the GCIO's *Internal Review* and the BCPSA's *Privacy Breach – Human Resources Review*, the government determined that the employee was not authorized to take home the personal information of MHSD and MCFD clients.[5] I agree and I find that a privacy breach did occur at MHSD and at MCFD.

The privacy breach response

[46] In order to meet its obligations under s. 30 of FIPPA to protect personal information once a breach has occurred, a public body must determine the steps necessary to mitigate any harm or potential harm caused and ensure the breach will not be repeated.

[47] The four key steps in responding to a privacy breach are:

1. Contain the breach;
2. Assess the risk of harm;
3. Determine whether notification is required; and
4. Develop prevention strategies.

[48] For greatest effectiveness, the first three steps should be taken simultaneously or in quick succession.

---

[5] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*, Ministry of Public Safety and Solicitor General, January 29, 2010. See Finding #3, p. 15. *Internal Review – Privacy Breach, Ministries of Housing and Social Development & Children and Family Development*, Office of the Chief Information Officer, January 29, 2010. See p. 10.

[49] **Contain the Breach**—Public bodies should take all reasonable steps to stop or limit a breach. Depending on the circumstances, this may include recovering lost or stolen records, reporting thefts to the police, revoking database access or simply stopping an unauthorized practice.

[50] In this case, the MHSD breach was effectively contained when the RCMP removed computers and the government documents from the employee's home. MHSD had already halted the practice of using caseload reports in May 2007. No further action to contain the breach was required by MHSD.

[51] As for MCFD, the RCMP intervention did not serve to completely contain the breach. When the employee returned to work, many questions about his arrest and his potential risk to information security remained unanswered. MCFD did not ask why its employee was holding two year old documents containing sensitive personal information. MCFD was unable to identify documents printed by its own employees. Without clear answers from the RCMP regarding the nature of its investigation, the employee should not have had his system access reinstated. At the very least, close monitoring of the employee's access should have continued until MCFD received the answers to its questions. I agree with the comments of Bert Phipps, who authored the BCPSA review,[6] on this situation:

> The managers responsible for him did not have enough detail about the situation in order to make an informed decision about his return to that position. They relied primarily on their perception of him as a diligent employee. They should have sought more information from the employee, the GSO and the police, and made more enquiries about the sample document which the police had provided.

[52] While MCFD made some initial efforts to contain the breach, the investigative process and justification for reinstating the employee's systems access was weak and appeared ad hoc. Based on the circumstances, I find the steps taken by MCFD to contain this breach were not adequate.

[53] **Risk Assessment**—Appropriately assessing the risk is crucial to determining whether further action is required to mitigate harm. The sensitivity of personal information is related to the potential for harm or hurt that might attach to the identification of an individual because of the nature of the information. The following are some of the factors public bodies should consider when assessing risk:

1. What kinds of personal information are involved?
2. What format was the information in (paper, electronic)?

---

[6] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*, Ministry of Public Safety and Solicitor General, January 29, 2010. See Finding #8, p. 17.

3. Was it protected (encrypted, anonymized, password protected)?
4. Was the breach accidental or deliberate?
5. Can the personal information be misused?
6. Was the breach an isolated event or is there a risk of ongoing or further exposure?
7. Who and how many individuals are affected by the breach?
8. Is there a relationship between the unauthorized recipients and the data subject? A close relationship between the victim and the recipient could increase the likelihood of harm.
9. Is there risk to public health and/or safety as a result of the breach?
10. Has the information been recovered?

[54] In this case, the personal information was very sensitive and was not adequately protected. It seems a fair assumption to assume that the "prospect of criminal activity or other intentional wrongdoing" was considerable. The personal information at risk in this case included:

- Client names;
- Addresses;
- Birth dates;
- Social Insurance Numbers;
- Personal Health Numbers;
- Benefit Category (*e.g.* single parent); and
- Spouses' names.

[55] One mitigating factor is that the RCMP tested a sample of the records and found no indication of financial fraud or identity theft. Despite this assurance, this breach created a very high risk of harm to those affected. Accordingly, notification was necessary without delay.

[56] Therefore, once it was determined that a privacy breach had occurred, I find that MHSD and MCFD correctly considered the risk of potential harm to be high and proceeded with notification in an effort to prevent harm or mitigate further harm.

[57] **Notification**—Giving notice to affected individuals is often the most important step in responding to a privacy breach. In Order F07-01,[7] the former Commissioner explained the timing and purpose of notification:

[7] [2007] B.C.I.P.C.D. No. 1.

> [36] A number of groups may require notification following a privacy breach. The most important of these are the affected individuals. An important purpose of notification of affected individuals was described in Investigation Report F06-01:
>
> > [106] …In my view, the key (but not sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed.
>
> [37] In this light, notification to be effective must be given in a timely enough fashion to allow those affected to effectively mitigate the breach's risks. The reasonableness of the timing is measured by whether it is objectively diligent and prudent in all the circumstances.

[58] The most significant failure in the ministries' response to this breach is the length of time they took to notify affected individuals of the privacy breach. Approximately seven months passed from the date of the RCMP's discovery until the notifications were mailed. It is clear, beyond any doubt, that affected individuals should have been notified within days of the April 7, 2009, discovery. A seven-month delay in notification meant that any reasonable opportunity for risk mitigation was lost. Accordingly, by delaying notification for over seven months the MHSD and MCFD failed to meet their obligations under s. 30 of FIPPA.

[59] I note that when MHSD did issue its initial notification, a further privacy breach occurred when the breach notification letters were sent to the wrong addresses.

[60] **Prevention Strategies—**In order to recommend prevention strategies it is necessary to understand the cause or causes of the failure to respond appropriately to this privacy breach. The essential problem with the MCFD and MHSD responses to this breach was that an alarming number of government employees, ranging from investigators, to managers, to directors, did not recognize that there was a potential privacy breach. In total, at least 26 different employees[8] had sufficient information to determine that a privacy breach had occurred. Based on our investigation, it appears that only two of the 26 employees recognized that a breach had occurred. However, these two individuals failed to take effective action to ensure that the matter was brought to the attention of the appropriate executive member within their ministry. An effective response to the breach did not occur until the matter was finally reported to the Minister of Citizens' Services on October 20, 2009, by the head of the BCPSA.

---

[8] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*, Ministry of Public Safety and Solicitor General, January 29, 2010. See Finding #7, p. 17.

[61] I acknowledge that the RCMP and PLMS investigations appeared to divert the focus away from the privacy issue and resolving the issue of the employee's alleged false identities became the priority. This caused crucial information to be held back from senior decision makers as late as August 2009. In addition, the statement by the employee's manager that he was authorized to have the documents at home also caused a delay in recognizing that a breach had occurred. Finally, there appears to have been a belief by public servants that they could not take any further action while the RCMP and PLMS investigations were underway.

[62] I find the following factors contributed to the initial breach and to the ministries' failure to respond appropriately to this privacy breach:

1. There was a significant lack of knowledge and understanding in both ministries of the rules respecting the protection of personal information resulting in a general inability of public servants to recognize a potential privacy breach.

2. The government policies and procedures that apply in a privacy breach situation do not use the word "privacy" and do not provide guidance on how to determine if a privacy breach has occurred. As a result it is difficult, if not impossible, for public servants to find the appropriate policy when dealing with a privacy breach.

3. Too many public servants are not hearing the government's message about the need to protect personal information. Knowing who to turn to should be second nature.

Creation of an executive-level Chief Privacy Officer

[63] The government business of collecting and using personal information is becoming more complex and the security risks are constantly evolving. In this environment, maintaining the security of personal information requires that the government constantly review, revise and communicate its privacy-related business practices. As this case and others investigated by this Office have indicated, the government's current strategy to protect personal information appears ineffective.

[64] In 2006, the OIPC investigated a privacy breach caused by the sale of un-wiped government computer backup tapes. Then Commissioner Loukidelis identified "systemic failures" when examining the government's personal information security.[9] In the 2007 EDS breach investigation, the Commissioner found the personal information security arrangements and the nine month delay

[9] [2006] B.C.I.P.C.D. No. 7, Sale Of Provincial Government Computer Tapes Containing Personal Information, March 31, 2006. This breach involved the personal information of thousands of individuals.

in notifying the affected individuals was a failure to comply with s. 30 of FIPPA.[10] Finally, in a more recent case, the OIPC investigated the 2008 loss of personal health information on Ministry of Health Services computer tapes. The investigation found that "the Ministry's policies and practices resulted in failure to ensure the tape loss was detected in a timely way" and the affected individuals were not notified in a timely manner.[11]

[65] This case provides an example of a ministry that collects some of the most sensitive personal information in all of government, yet at the level where it matters most some of the fundamental principles of privacy were either unknown or ignored. The privacy message is not getting through to many public servants who deal with personal information on a daily basis.

[66] The GCIO recommended:

> Establish a central authority within the GCIO with overall responsibility for managing information incidents including policy, audit, investigations and police liaison.[12]

[67] While I agree with the need to establish a central privacy authority, in my view this authority must accomplish more than managing and responding to information incidents. The provincial government urgently needs a central and visible authority to direct the provincial government's privacy-related functions and to create and foster a culture of privacy through policy making, advocacy and education.

[68] I agree with Bert Phipps' finding that, "there were a number of organizational and cultural factors which contributed to the failings in judgement".[13] The human resources and the privacy staff were taking part in organizational adjustments and experiencing shifts in leadership. On top of this was a lack of clarity regarding the obligations and restrictions imposed by FIPPA, which may have caused government workers to be uncertain about what they can acquire, use or disclose about another employee. A Chief Privacy Officer ("CPO") with the authority to direct the provincial government's privacy-related functions would represent visible and accessible leadership for public servants faced with similar uncertainties.

---

[10] [2007] B.C.I.P.C.D. No. 13. This breach affected 94 individuals.
[11] [2008] B.C.I.P.C.D. No. 16. This breach involved 124 patients and 570 physicians.
[12] "*Internal Review, Privacy Breach Ministry Of Children And Family Development, Ministry Of Housing And Social Development"*. See Appendix A of this report for the text of all of the recommendations.
[13] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*, Ministry of Public Safety and Solicitor General, January 29, 2010. See Finding #9, p. 21.

[69] Public trust in the government's commitment to protect personal information requires meaningful investments in personal information security. Meaningful investments require a focused, coordinated approach to deliver a consistent message across government. However, meaningful investments will not be effective as long as privacy remains tied to information management or security. Investments in privacy will only be meaningful and effective when government recognizes privacy as an issue distinct from other information security issues. The GCIO has recommended that a central authority within his office be established to manage information incidents. To most effectively do this, the government must, in my respectful opinion, immediately create an executive-level position of CPO. I believe that to do so would create a bright light of assistance for those public servants across the government who have to manage personal information while respecting privacy and, at the same time, to quickly and effectively deal with privacy breaches if they occur.

[70] The executive-level position of CPO I recommend would be the "central authority" recommended by the GCIO in his report; and, as a practical matter could be located in the GCIO office with the administrative and financial economies that would provide. However, it is in my view, essential the CPO have executive and visible decision-making authority with respect to matters of privacy. A CPO would provide the following benefits, among many others, to the government and the people of British Columbia:

- Develop a government-wide strategic vision and goals for privacy;
- Create and coordinate an educational program to foster privacy, security awareness and compliance within government;
- Develop a coordinated response to privacy breaches;
- Establish government-wide privacy training standards and oversee training;
- Conduct ongoing privacy compliance monitoring; and
- Collaborate with relevant government stakeholders to ensure government compliance with FIPPA.

[71] Attached as Appendix C is a full list of the central responsibilities a meaningful and effective CPO position would have.

[72] **Recommendation #1:** For these reasons, I recommend that government create an executive-level CPO to direct the provincial government's privacy-related functions.

Revise Core Policy and Procedures to create distinct privacy policy

[73] Currently, privacy issues in the Core Policy and Procedures Manual are considered a part of the information management and loss management policies

and procedures. Apart from the policy titled, Information Management and Information Technology Management[14] references to personal information are rare and references to privacy are non-existent. On the procedures side, Loss Reporting[15] provides the reporting requirements for a "loss incident" or "information security incident". The loss reporting procedures do not mention the loss of personal information or the term privacy breach. Consequently, the Core Policy and Procedures Manual provides no assistance in recognizing a privacy breach or how to respond to a privacy breach.

[74] As I mentioned in the first recommendation, it is imperative that the government recognize privacy and privacy-related issues as distinct from information management issues.

[75] **Recommendation #2:** I recommend that the Core Policies and Procedures Manual be revised to include a separate chapter outlining the principles of privacy, the government's privacy obligations under FIPPA and the government's policies and procedures for responding to privacy breaches.

Personal information security practices

[76] The GCIO made two recommendations with respect to improving personal information security practices:

> Consolidate and communicate corporate policies that provide direction to employees on how to manage, handle and ensure the security of personal information in their possession outside of the workplace.
>
> And
>
> Enhance information management processes at the Medical Benefits Program, Ministry of Children and Family Development to ensure adequate protection and security of personal information.[16]

[77] As noted above, I have found that both MCFD and MHSD failed to adequately secure personal information in their custody and control. In particular, neither public body had a system for ensuring that personal information removed from the office was tracked. In the case of MCFD, where the employee apparently was authorized initially to remove the personal information for work purposes, MCFD had no means of ensuring that the information was returned to the office in a timely fashion. For MHSD their information practices failed to ensure that when reports were no longer required, they were accounted for and securely destroyed.

---

[14] Chapter 12, Core Policy and Procedures Manual.
[15] Section L, Core Policy and Procedures Manual.
[16] *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency*. See Appendix B of this report for the text of all of the recommendations.

[78] **Recommendation #3:** I recommend that MHSD enhance information management processes to ensure adequate protection and security of personal information.

Criminal record checks

[79] With respect to Bert Phipps' recommendations in his report, *Privacy Breach - Human Resources Review, Ministry Of Children And Family Development, Ministry Of Housing And Social Development*, *BC Public Service Agency* (see Appendix B), the weaknesses he identified in the criminal record check process related to a policy that was replaced in March 1, 2009. Therefore, I do not agree that the facts of this privacy breach support recommendations for expanding criminal record checks.

5.0 RECOMMENDATIONS

[80] In summary I recommend:

1. That the government create an executive-level CPO to direct the provincial government's privacy-related functions.

2. That the Core Policies and Procedures Manual be revised to include a separate chapter outlining the principles of privacy, the government's privacy obligations under FIPPA and the government's policies and procedures for responding to privacy breaches.

3. That MHSD enhance information management processes to ensure adequate protection and security of personal information.

6.0 CONCLUSIONS

[81] In some situations the best legislation, policies and preventive measures may not prevent a determined employee from taking government documents home. However, this risk can be reduced if ministries ensure that they have in place reasonable security arrangements to protect personal information. That was not the case here.

1. MHSD did not make reasonable security arrangements, as required by s. 30 of FIPPA, to protect the personal information in the caseload reports.

2. MCFD did not make reasonable security arrangements, as required by s. 30 of FIPPA, to protect personal information when it authorized an employee to take government documents out of the workplace.

[82] When a breach of FIPPA occurs, public bodies must continue implementing reasonable security arrangements to ensure they make every reasonable effort to prevent or mitigate harm to the affected individuals. For the reasons pointed out earlier, this did not happen.

3. MCFD failed to make every reasonable effort to contain the breach.

4. MHSD and MCFD failed to make every reasonable effort to provide notification without delay.

[83] The results of this investigation and the investigations of the GCIO and the PSA illustrate that government has not yet established a culture of privacy. This must be a goal of government and in order to achieve this goal government must demonstrate that privacy is distinct from and as important as other security concerns.

[84] I am grateful for the assistance of the GCIO, which generously accepted my investigators' participation in interviews arranged by the GCIO and provided whatever documentation was requested of them. I am also grateful to all those individuals who answered our questions and offered their own solutions.

[85] Patrick Egan, Portfolio Officer and Justin Hodkinson, Portfolio Officer, conducted this investigation and prepared this report.

February 8, 2010

ORIGINAL SIGNED BY

Paul D.K. Fraser, Q.C.
A/Information and Privacy Commissioner
for British Columbia

OIPC File No: F09-40015

Appendix A

INTERNAL REVIEW
PRIVACY BREACH
Ministries of Housing and Social Development &
Children and Family Development
January 29, 2010

RECOMMENDATIONS

Recommendation 1: *Establish a central authority within the GCIO with overall responsibility for managing information incidents including policy, audit, investigations and police liaison*

Recommendation 2: *Enhance education and training to ensure all employees are aware of information privacy management obligations and practices*

Recommendation 3*: Ensure human resource incident investigations or reviews involving government information, include timely consultation and information management direction from the GCIO*

Recommendation 4: *Consolidate and communicate corporate policies that provide direction to employees on how to manage, handle and ensure the security of personal information in their possession outside of the workplace*

Recommendation 5: *Enhance information management processes at the Medical Benefits Program, Ministry of Children and Family Development to ensure adequate protection and security of personal information*

Recommendation 6: *Align investigation processes established by the Prevention and Loss Management Services Branch, Ministry of Housing and Social Development with corporate policies*

Appendix B

PRIVACY BREACH
HUMAN RESOURCES REVIEW
Ministry of Children and Family Development
Ministry of Housing and Social Development
BC Public Service Agency
January 2010

RECOMMENDATIONS

1. The BC Public Service Criminal Records Check Policy should be reviewed, in consultation with the Government Chief Information Officer, with an eye to expanding the types of positions which are considered for designation as subject to a criminal records check. In particular, positions which provide access to personal information systems should be considered.

2. In the longer term, as technology advances, the BC Public Service Agency and the Ministry of Public Safety and Solicitor General, should explore ways to enhance the thoroughness and integrity of background checks.

3. A new human resource policy should be introduced to complement the current Criminal Records Check Policy. This new policy would mandate the steps to be taken when a government employee is arrested, charged, or convicted of a criminal offence.

4. The Ministry of Children and Family Development and the BC Public Service Agency should confirm the transition plan for human resource services, to ensure clarity in the respective roles and responsibilities of Strategic Human Resources and the BC Public Service Agency.

5. Following a review of this report, and the companion report on the privacy breach, the Ministry of Children and Family Development should review the judgement exercised by the managers involved and identify remedial action to ensure managers have the direction, training and support to respond more effectively to complex issues.

6. The Deputy Ministers' Council should review how external investigative agencies link with government when public servants are the subject of a criminal investigation. The aim of the review would be to ensure that the right information gets to the right people in government in a timely manner, while simplifying the process for police and other enforcement agencies.

Appendix C

DUTIES OF THE CHIEF PRIVACY OFFICER

1. Develop and maintain the government's strategic vision and goals for privacy in consultation with stakeholders inside and outside of the provincial government.

2. Lead development and implementation of a comprehensive, coordinated approach to privacy protection and compliance across the provincial government.

3. Assist where appropriate with privacy impact assessments of legislative, policy and program proposals involving collection, use or disclosure of personal information (including those involving integration, sharing or linkages of information systems or databases containing personal information).

4. Ensure that technologies sustain, and do not erode, privacy protections relating to the collection, use and disclosure of personal information.

5. Participate in the development, review and updating of government-wide privacy-related policy, procedures and guidelines, including providing advice and guidance on privacy issue in contracts, information-sharing agreements, research agreements and other relationships involving the collection, use or disclosure of personal information (including developing sample agreement language).

6. Direct responses to privacy incidents as they emerge and direct investigations of privacy incidents with a view to assessing risk and identifying measures to be implemented to reduce risk of recurrence.

7. Establish privacy training standards and oversee ongoing training and education of government employees regarding privacy responsibilities at law and under government policy and procedures.

8. In collaboration with relevant stakeholders within government, including the GCIO encourage and support government compliance with the privacy requirements under the FIPPA and all other applicable laws respecting personal information.

9. Conduct periodic privacy risk assessments and conduct ongoing privacy compliance monitoring activities in coordination with the government's other compliance and audit functions.

10. Collaborate with the GCIO in performing periodic information security risk assessments and conduct ongoing monitoring activities in coordination with the government's other compliance and audit functions.

11. Serve as the designated point of contact with the OIPC for matters relating to privacy compliance under FIPPA.

12. Report publicly at least annually on the activities of the CPO, including information about complaints and about privacy incidents.

13. Maintain a publicly-available website and post to it in a timely fashion policies, procedures, completed privacy impact assessments and other information and records produced or compiled by the CPO in performing her or his duties.

Appendix D

Glossary

BCPSA	The BC Public Service Agency provides human resource services to all ministries.
EAW	An Employment Assistance Worker assists individuals on income assistance.
Encryption	Encryption is a means of concealing information contained in an electronic format by means of a code or cipher.
FIPPA	The *Freedom of Information and Protection of Privacy Act* is the legislation that governs the collection, use, disclosure and security used in relation to personal information under the custody or control of public bodies, including the provincial government.
GCIO	The Government Chief Information Officer is responsible for the creation and implementation of information security standards.
GSO	The Government Security Office is within the Risk Management Branch of the Ministry of Finance. This office is responsible for identifying and mitigating potential risks across government.
MCFD	The Ministry of Children and Family Development delivers a range of services, including child protection, youth justice, adoptions, child care, early childhood development and services for special needs children and youth.
MCFD ISO	The Ministry of Children and Family Development Information Security Officer is responsible for the management and security of information technology within the ministry.
MCIO	Each ministry has a Ministry Chief Information Officer, who is responsible for records management, security and electronic service delivery.
MHSD	The Ministry of Housing and Social Development delivers employment and income assistance services and provides strategic advice about housing issues.

MIS	The Management Information System is an electronic database shared by MCFD and MHSD.
OIPC	The Office of the Information and Privacy Commissioner monitors and enforces FIPPA.
PHNs	Personal Health Numbers are issued by the British Columbia provincial government's Ministry of Health Services and are used to identify British Columbia citizens when they access our public health system.
PLMS	Prevention and Loss Management Services is a department within MHSD. PLMS staff conducts investigations into potential fraudulent claims and employee misconduct.
Privacy Breach	A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information that is in the custody of or under the control of a public body.
RCMP	Royal Canadian Mounted Police.
Screen prints	Screen prints are computer screen printouts from the MCFD data system, known as the Management Information System.
SIN	Social Insurance Number.
Strategic HR	Strategic Human Resources. Provides advice on workforce planning, employee engagement and organizational development.