

Internal Review

Privacy Breach

Ministries of Housing and Social Development &
Children and Family Development

Office of the Chief Information Officer
Ministry of Citizens' Services
January 29, 2010



The Internal Review

On October 21, 2009, the Honourable Ben Stewart, Minister of Citizens' Services asked the Government's Chief Information Officer (GCIO) to undertake an internal review of the privacy breach involving clients of the ministries of Housing and Social Development (MHSD) and Children and Family Development (MCFD). This report documents the conclusions, findings and recommendations of the internal review.

The GCIO's internal review is one of three reviews. The BC Public Service Agency (BCPSA) was assigned an examination of human resource policies and practices related to the privacy breach to the Ministry of Public Safety and Solicitor General. The Information and Privacy Commissioner for British Columbia launched a separate investigation into the privacy breach.

The Events

The events surrounding the privacy breach occurred over a period of several months between April 7, 2009, when an employee with the MCFD was arrested by the RCMP on suspicion of identity falsification, and early December 2009, when all affected clients of the ministries of MHSD and MCFD received breach notification letters.

Following the arrest of the MCFD employee, the RCMP searched the employee's home and seized documents, as well as several computers, data storage devices and equipment that could be used for fabricating identification. Records seized included 408 pages containing names, birth dates, and social insurance numbers. The next day, the RCMP provided the Risk Management Branch, Ministry of Finance, the government office responsible for liaison with the police, with a sample page from a 2007 "Caseload Management Report" illustrating the documents contained the personal information of government clients. The document presented contained no clear indication of which Ministry owned the document. Risk Management Branch contacted MCFD, the ministry responsible for the employee, expressing concerns that sensitive documents were found at the employee's home. The Risk Management Branch believed, because of its confidential liaison role and concerns about possibly compromising a police investigation, it was limited in what information it could share. When contacted by MCFD directly, the RCMP also provided only limited information. Because of reassurances from MCFD, the Risk Management Branch did not realize the personal information of MCFD and MHSD clients was potentially at risk, nor was any contact made with MHSD regarding the records.

With regard to the delay in notifying MCFD clients, a factor contributing to the failure of early identification of the privacy breach related to verification that the employee could work at home and have this type of information. Due to this understanding, i.e., that it was appropriate for the employee

to have access to these records for work purposes, MCFD managers assessing the employee's access to this information did not appear to adequately consider the extenuating circumstances of the investigation and the employee's past criminal history.

With regard to MHSD, it was not until July, when the RCMP provided the records to MCFD, that it was recognized that a large number of records belonged to MHSD and that a privacy breach of MHSD records had occurred. Then, the decision to suspend the privacy work, so as not to compromise the criminal investigation, was based on a draft protocol that did not align with corporate policy.

The entire course of events is illustrative of a series of missed opportunities and inaction, related to gaps in information, mistaken assumptions, limited knowledge, and insufficient awareness in related program areas.

The Findings and Recommendations

<i>Findings</i>	<i>Recommendations</i>
Incident Management and Investigations	
Insufficient response and lack of effective communication, coordination and information sharing between employees, ministries and law enforcement	Recommendation 1: <i>Establish a central authority within the GCIO with overall responsibility for managing information incidents including policy, audit, investigations and police liaison</i>
Corporate Information Management	
Lack of knowledge of policies and practices regarding information privacy protection requirements	Recommendation 2: <i>Enhance education and training to ensure all employees are aware of information privacy management obligations and practices</i>
Lack of clear policy direction regarding information management and security practices for employees	Recommendation 3: <i>Ensure human resource incident investigations or reviews involving government information, include timely consultation and information management direction from the GCIO</i>
	Recommendation 4: <i>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</i>
Ministry Information Management Policy and Practice	
Inadequate knowledge and application of information and privacy security practices	Recommendation 5: <i>Enhance information management processes at the Medical Benefits Program, Ministry of Children and Family Development to ensure adequate protection and security of personal information</i> Recommendation 6: <i>Align investigation processes established by the Prevention and Loss Management Services Branch, Ministry of Housing and Social Development with corporate policies</i>

Table of Contents

1.0 Introduction 4

2.0 Background, Purpose and Approach 5

3.0 Incident Summary and Event Timeline 7

4.0 Observations & Conclusions 13

5.0 Findings & Recommendations 15

Appendices 18

Appendix 1 - Terms of Reference

Appendix 2 – Detailed Listing of Documents Found

Appendix 3 – Program Areas Involved

Appendix 4 – Policy Overview

1.0 Introduction

On October 21, 2009, the Minister of Citizens' Services, the Honourable Ben Stewart, requested the Government Chief Information Officer (GCIO), Ministry of Citizens' Services (MCS), undertake an internal review and investigate a privacy breach involving clients of the ministries of Housing and Social Development (MHSD), and Children and Family Development (MCFD). The Terms of Reference for this review, dated November 23, 2009, are included as Appendix 1.

The contents of this report documents the results, findings and recommendations including a summary of events that transpired and the action taken or, in some cases, inaction by government employees in the related program areas in the management of the privacy breach.

The GCIO's internal review is one of three reviews. A second review involves the Information and Privacy Commissioner for British Columbia, who as an independent officer of the legislature launched a separate investigation into the privacy breach. A third involves an examination, led by the BCPSA and assigned to the Ministry of Public Safety and Solicitor General, of human resource policies and practice in this case.

This reports provides six recommendations, all of which government is committed to implementing.

The Freedom of Information and Protection of Privacy Act (FOIPP Act) governs privacy and access in the B.C. Public sector. The FOIPP Act provides the public with a right of access to information held by public bodies while balancing that right with stringent rules to protect the privacy rights of individuals. The FOIPP Act has strict rules governing personal information that authorizes its collection, use and disclosure only in specified circumstances.

The Minister of Citizens' Services is responsible for the FOIPP Act. The Government's Chief Information Officer, under the direction of the Deputy Minister, Citizens' Services, provides leadership, support and services to ministries and other public bodies to assist them in complying with their privacy and access obligations with regard to the FOIPP Act. It also manages the legislative change process for the Province's privacy and access legislation and provides corporate privacy advice. The Chief Executive Officer, Shared Services BC, through the Information Access Operations branch, is responsible for supporting ministries in meeting their operational records access and privacy needs while individual ministries and programs are responsible for ensuring measures are implemented to meet the requirements of the FOIPP Act.

2.0 Background, Purpose and Approach

2.1 Background

On April 7, 2009, a government employee was arrested at MCFD offices by the RCMP under suspicion of identity falsification. The employee's home was searched and government documents, computers, data storage devices and equipment, which could be used for fabricating identification, were seized. Police action on April 7, 2009, and the months following, led to a number of events including the recognition of a privacy breach involving over 1,400 clients of MCFD and MHSD.

2.2. Purpose

The purpose of this internal review is to determine the circumstances that led to the delay in categorizing this incident as a privacy breach and the reasons why government managers did not, at the outset of this incident, take appropriate steps to minimize potential risks to clients of MCFD and MHSD, as well as safeguard additional personal information the employee continued to access through employment.

A privacy breach is a collection, use, disclosure, disposal, or storage of personal information as well as access to that information, whether accidental or deliberate, that is not authorized by the FOIPP Act.

Personal Information, as defined under the FOIPP Act, means "recorded information about an identifiable individual" other than "contact information" (information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual).

2.3 Approach

The approach taken included:

- conducting over 30 interviews with deputy ministers, assistant deputy ministers, senior managers and supervisors from the ministries of HSD, CFD, Finance, CS and BCPSA;
- discussing events with the RCMP;
- gathering and reviewing documentary evidence;
- reviewing the employee's systems and email activities;
- identifying and analyzing relevant legislation, policies, practices and systems protocols; and,
- reviewing emails, communications and notes submitted by interviewees.

To ensure transparency during the internal review process and reduce redundancy between reviews, staff from the Office of the Information and Privacy Commissioner for British Columbia observed government's investigation, including attending various meetings and interviews.

The chronologies, findings, recommendations and references recorded in this report reflect to the best of the reviewers' abilities the events that transpired, based on the information provided verbally and in written documents.

3.0 Incident Summary and Event Timeline

3.1 Incident Summary

On October 16, 2006, the employee joined Office 107, MHSD, formerly known as the Ministry of Employment and Income Assistance, Victoria. As a condition of employment, the employee was required to complete a criminal record check. On October 1, 2007, the employee transferred to MCFD as a Supervisor in the Medical Benefits Program, Children and Youth with Special Needs Operations, Provincial Services.

On February 26, 2009, the Security Officers, Risk Management Branch, Ministry of Finance, responsible for coordinating police liaison, were contacted by the Special Investigations Unit, Insurance Corporation of British Columbia (ICBC), and advised that a government employee was under investigation for identity falsification. In early March, ICBC transferred the investigation to the RCMP. On April 7, 2009, following coordination by the Security Officers, Risk Management Branch, the RCMP arrested the employee at MCFD offices. The RCMP also searched the employee's home and seized documents, several computers, data storage devices and equipment that could be used for fabricating identification. The employee was questioned and released pending further investigation. The employee's systems access was suspended by Workplace Technology Investigations, Shared Services BC, MCS, at the request of MCFD.

On April 8, 2009, the Security Officers, Risk Management Branch, Ministry of Finance, were advised by the RMCP that records seized in the employee's home included names, birth dates, and social insurance numbers (appendix 2 includes a detailed list). The next day, the RCMP provided the Risk Management Branch with a sample page from a 2007 "Caseload Management Report" illustrating that the documents contained the personal information of government clients. The document presented contained no clear indication of which Ministry owned the document. Because the employee in question worked for MCFD, the security officers contacted the Director, Strategic Human Resources, MCFD, with concerns that sensitive documents were found at an employee's home; no contact was made with MHSD at that time. The security officers, due to their confidential liaison role and because of concerns regarding possibly compromising a police investigation, believed they were limited in what they could share about the investigation with Strategic Human Resources, MCFD. The security officers, while concerned about the records being in this employee's hands generally, did not identify that there was a potential privacy breach because of reassurances from MCFD.

On April 8, 2009, the Senior Director, Medical Benefits Program, MCFD, contacted the RCMP. The RCMP did not confirm to MCFD, nor deny, if criminal charges would be laid or what materials were seized. They indicated the matter involved the employee falsifying identification.

On April 8, 2009, the employee began an absence from work, initially at the direction of the employer, and later because of illness, which continued until April 24, 2009.

On April 14, 2009, the employee's Manager, Medical Benefits Program, MCFD met with the Director, Strategic Human Resources, MCFD, to discuss the "Caseload Management Report" sample page provided by the police. The manager was asked about the type of information found in the employee's home. Even though it is unclear whether or not the manager reviewed the document at all, the manager confirmed that the employee was permitted to work at home and have this type of information. No attention was drawn by either the manager or Director, Strategic Human Resources, MCFD, that the report was from MHSD and not MCFD. The Director, Strategic Human Resources then advised the Security Officers, Risk Management Branch, of the employee's authorization to work at home and, based on this information, no further action was taken with respect to the document.

On April 27, 2009, the employee returned to work and his systems access was restored; a week earlier, the employee's email had been reactivated. The Director, Strategic Human Resources, MCFD, expressed concerns with the employee's continued systems access. As a result, a Labour Relations Specialist at the BCPSA advised the Director, Strategic Human Resources and the Senior Director, Medical Benefits Program that, where there is a reasonable concern to believe an employee poses a threat to databases, the employee needs appropriate supervision. Failing this measure, the specialist advised that the employee's systems access can be removed or the employee can be suspended pending the outcome of the investigation.

As part of addressing concerns regarding the employee's systems access, the employee's manager assured the Senior Director, Medical Benefits Program, that the employee's work would be overseen and any inappropriate use of the systems identified. The employee's manager implemented a tracking document to record the employee's daily work activities and met with the employee daily. After about a month, the manager discontinued use of the tracking documents believing it was repetitive of the daily meetings held with the employee.

On May 20, 2009, the employee, accompanied by a union representative, was interviewed by a BCPSA Human Resources Consultant and the Senior Director, Medical Benefits Program, MCFD, about his removal from the workplace by police and because, following an audit of his email, it had been determined that the employee was using government's email for personal school work. This meeting occurred over three weeks after the employee returned to work. The consultant and senior director determined that there was insufficient information available to pursue disciplinary or other measures against the employee, with the exception of a verbal warning with regard to the employee's email use.

On July 9, 2009, Security Officers, Risk Management Branch, met with the RCMP and discussed continuing concerns about the sensitive information found in the employee's home. The RCMP confirmed that, on a sampling of personal information contained in the documents, no evidence of identity theft or fraud had been found. The Security Officers referred the RCMP to the Ministry Information Security Officer, MCFD, to follow up on the documents.

On July 13, 2009, the RCMP advised MCFD's Information Security Officer that, in the past, the employee had been convicted of criminal activity, that he had been in trouble for counterfeiting identifications,

and that the RCMP was concerned with the employee's use of different names. The next day, as a result of the discussion, the RCMP provided MCFD's Information Security Officer with the documents seized from the employee's home. The MCFD's Information Security Officer contacted the Senior Security Analyst, Workplace Technology Investigations, who recommended suspension of the employee's access again. There was a discussion between the RCMP and MCFD's Information Security Officer. Subsequently, Workplace Technology Investigations was requested by the information security officer to remove their Senior Security Analyst from the case as it was believed that the Workplace Technology Investigations analyst was pre-judging the level of incident severity.

On July 13, 2009, MCFD's Information Security Officer discussed the potential breach with a Senior Advisor, Information Access Operations (IAO), Shared Services BC, MCS, responsible for MCFD privacy. The privacy advisor advised that it would be a privacy breach if the employee was not authorized to view this information.

On July 15, 2009, MCFD's Information Security Officer met with the Director, Strategic Human Resources, MCFD, and determined that a large number of the documents appeared to be from MHSD, and a smaller number from MCFD.

On July 20, 2009, MCFD's Information Security Officer met with a Senior Advisor and a Senior Privacy Analyst, IAO, responsible for MHSD privacy and reviewed the documents. As a result of the meeting, the Senior Advisor wrote to MHSD's Executive Director, Strategic Human Resources, stating that this was a privacy breach and that, once the breached records were obtained from MCFD, the breach should be reported to the Office of the Information and Privacy Commissioner for British Columbia. Despite being aware of the need to report privacy breaches to the GCIO, the Senior Advisor did not contact the GCIO, claiming uncertainty with the new organizational structure of the GCIO's Knowledge and Information Services Branch. The Office of the Information and Privacy Commissioner for British Columbia was not notified.

The Senior Advisor, IAO, expected to take appropriate steps regarding the breach once they received and reviewed the MHSD documents from MCFD. However, the Senior Advisor did not receive the MHSD documents immediately as the MCFD Information Security Officer forwarded them to MHSD's Executive Director, Strategic Human Resources.

On July 27, 2009, MCFD's Information Security Officer met with the employee's manager and a Strategic HR Planner, Strategic Human Resources, MCFD. The group discussed that: a privacy breach investigation was underway at MHSD; a potential human resource investigation might be launched at MHSD; a RCMP investigation involving the employee was ongoing but charges had not been laid; there were concerns the employee was not being forthright about his identity; and, that the employee had a criminal record from 2006 for "fraud and identities".

At the July 27, 2009 meeting, it was agreed that the employee's manager would provide information from the meeting to the Assistant Deputy Minister (ADM) responsible for the Medical Benefits Program

area. A full briefing, including detailed background information about the employee, was not provided to the ADM or the manager's Senior Director. The manager did, however, obtain permission from the ADM to show the employee "the record". The next day, the manager sent an email to the July 27, 2009 meeting attendees that the employee was authorized to have the MCFD records at home and that, as such, the matter was not being pursued as a privacy breach at MCFD.

On July 27, 2009, following a discussion between MHSD's Executive Director, Strategic Human Resources and the Executive Director, MHSD's Prevention Loss Management Services (PLMS), a PLMS Investigator was assigned. The Investigator determined the employee had worked at MHSD; however, there was no valid reason for the employee, given his previous role at MHSD, to have the MHSD documents in his residence.

On July 30, 2009, the IAO Senior Advisor for MHSD privacy contacted the Executive Director, Strategic Human Resources, who advised that the records would be handed to PLMS the next day. Then, on July 31, 2009, the Executive Director, Strategic Human Resources, provided copies of documents to the PLMS Investigator. The Executive Director understood that IAO was the lead on the privacy breach and PLMS was the lead on the human resource investigation.

On August 4, 2009, the IAO Senior Advisor asked the Investigator, PLMS, for copies of the seized documents. On August 10, 2009, the Investigator conveyed to the Senior Advisor that copies of the documents would be provided and, on August 13, 2009, the Investigator transferred the documents to IAO. The next day, the PLMS investigation became a criminal investigation due to the suspected falsification of the employee's criminal record check, and paralleled the RCMP investigation. As MHSD turned the matter into a criminal investigation, IAO, following a draft MHSD protocol, suspended its privacy work to ensure that the investigation was not contaminated through privacy breach notifications. The MHSD draft protocol did not correctly align with corporate policy, which required notifying the GCIO of an information management security incident, including a privacy breach. Additionally, corporate policy requires an Investigator to consult with the Risk Management Branch and GCIO before contacting law enforcement authorities.

A briefing note, dated August 26, 2009, was prepared for the Assistant Deputy Minister, Regional Services Division, MHSD. It included information about the employee, his criminal records, the identification of fabrication equipment and MHSD documents seized from the employee's home. The note also referenced that there were no valid reasons for the employee to have these documents at his residence. The note indicated that IAO privacy staff were awaiting results of the criminal investigation before responding to the privacy breach, and that there was no evidence regarding misuse of records. One recommendation included in the briefing note was that PLMS advise MCFD of the progress of the investigation; this did not occur until October.

Based on the briefing note, the Assistant Deputy Minister, Regional Services Division, MHSD, understood that privacy staff were involved and that, while the employee did have clients' personal information, the records were from 2006-07, had been in the employee's possession all that time, and MHSD clients'

personal information had not been compromised. The ADM did not forward notification to MHSD's Deputy Minister or other senior government officials.

On October 15, 2009, PLMS briefed the Senior Director, Medical Benefits Program, MCFD, and a BCPSA Human Resources Consultant regarding the findings of the MHSD investigation. The employee was suspended.

On October 20, 2009, after being notified by staff, the Head of the BCPSA advised the Minister of Citizens' Services, responsible for the BCPSA and the *FOIPP Act*, that there was a potential human resource issue that involved personal information of over 1,400 government clients. The Minister of Citizens' Services' Ministerial and Executive Assistants were contacted by the Public Affairs Bureau. Public Affairs Bureau staff wanted to ensure that the Minister was aware of the issue in order to respond to any questions raised.

On October 20, 2009, the Minister of Citizens' Services' Ministerial Assistant contacted the Ministerial Assistants in MHSD and MCFD, who in turn advised their Ministers. The Head of the BCPSA also contacted the Deputy Ministers of MCS, MHSD and MCFD; by October 21, 2009, all were notified.

On October 21, 2009, the Government Chief Information Officer was notified by the Deputy Minister, MCS. The Head of the BCPSA, the GCIO and the Deputy Minister, MCS, met with the Minister of Citizens' Services. The Minister requested the GCIO undertake an internal review. The GCIO contacted the Deputy Ministers at MHSD and MCFD regarding the privacy breach.

The employee was dismissed on October 22, 2009. PLMS planned to interview the employee to gather more information but was unable to as the employee had already been terminated.

On October 25, 2009, staff with the GCIO prepared draft breach letters. These letters required confirming addresses of MHSD clients and review by the GCIO in consultation with MHSD and MCFD.

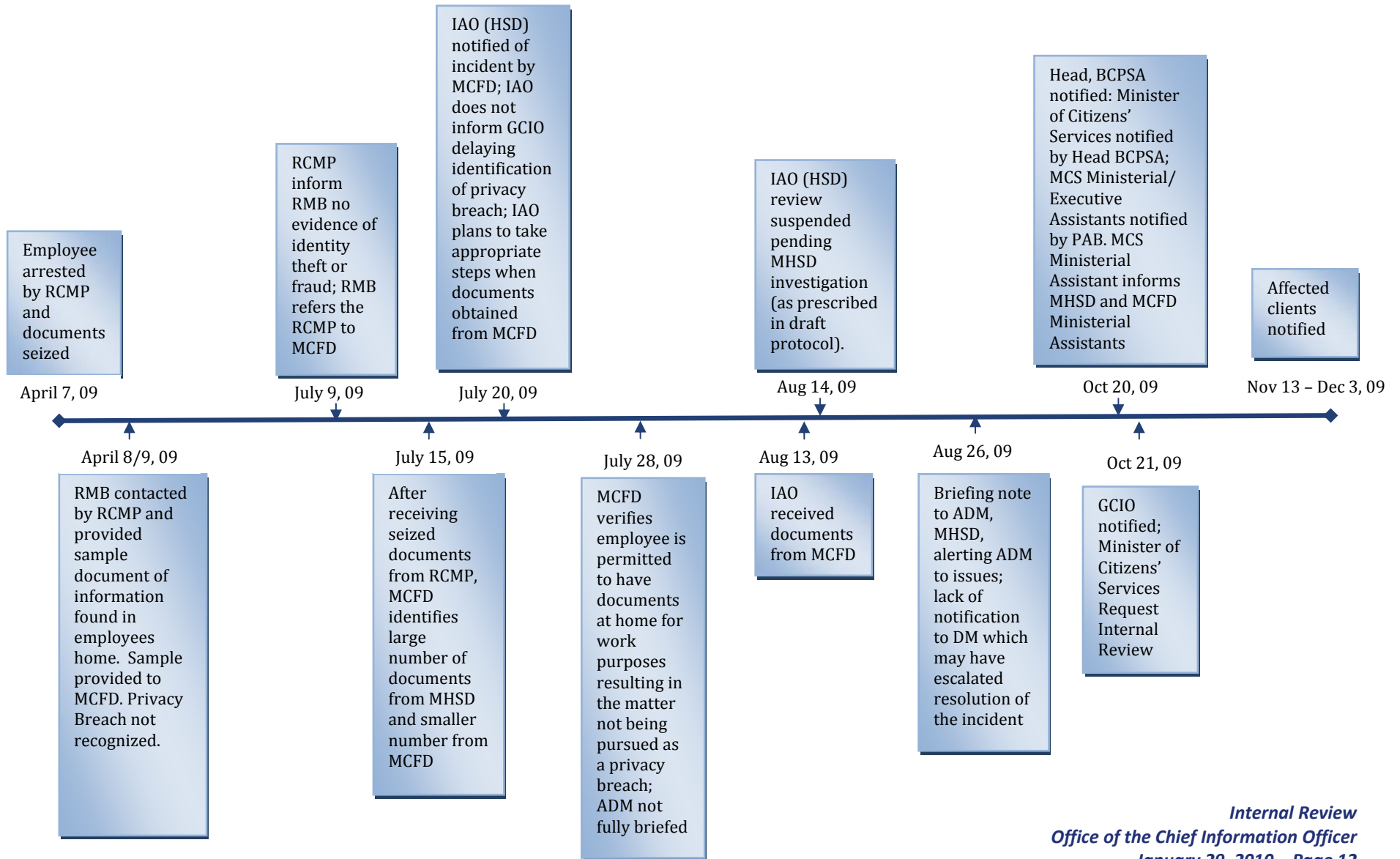
On November 13, 2009, the privacy breach notification letters were issued to MHSD clients.

On November 16, 2009, privacy breach notification letters were sent to MCFD clients.

On November 19, 2009, due to a clerical error, MHSD privacy breach notification letters were resent.

On December 3 and 4, 2009, MHSD clients previously unidentified were sent privacy breach notification letters.

3.2 Event Timeline



4.0 Observations & Conclusions

Information management problems began at the outset of this incident. Initially, when contacted by the RCMP in April 2009, Risk Management Branch, Ministry of Finance, while concerned about the issue generally, did not recognize that this represented a potential privacy breach. Based on the fact that the employee (who was under police investigation) was an MCFD employee, Risk Management Branch focused its efforts on notifying MCFD. Furthermore, based on its understanding of its police liaison role and concerns regarding possibly compromising a police investigation, Risk Management Branch believed that it was constrained due to confidentiality factors in the amount of information they could divulge. The expertise and knowledge with respect to government privacy obligations under the *FOIPP Act* was not sufficient at this stage to correctly identify the nature of the privacy incident and mitigate potential harm by taking corrective action. The degree of coordination and information-sharing between all parties involved in this matter was not sufficient to ensure that the privacy aspects of the incident were managed appropriately.

Other factors contributing to the failure of early identification of this privacy breach related to verification that the employee could work at home and have this type of information. As of April 2009, and throughout the period in question until a privacy breach was determined within MCFD in October 2009, a number of staff believed that it was appropriate for the employee to have these records for work purposes. Managers assessing the employee's access to this information did not appear to have considered the extenuating circumstances of the investigation, including the employee's past criminal history, nor was the responsible ADM provided a full briefing. Additionally and equally concerning is that the employee continued to have access to client information.

In July 2009, when the RCMP provided the package of seized documents to MCFD, it was realized that a large number of records also involved MHSD. MHSD, upon review of the documents, realized there was a privacy breach and, while a series of meetings, discussions and communications occurred towards managing the MHSD privacy breach, the GCIO was not notified due to a lack of judgment and awareness of policy.

Another contributing factor in the delay in notifying MHSD clients was the transfer of MHSD records to MHSD's privacy advisors, which was not completed in a timely way. Once this finally did occur in mid-August 2009, the privacy breach review was suspended to ensure that the MHSD criminal investigation was not compromised by privacy breach notifications. The decision to suspend notification to clients

was based on a draft protocol, which did not align with corporate policy direction. Information regarding the employee and the events was brought to the attention to the Assistant Deputy Minister within MHSD; however, it was not raised to the most senior level, the Deputy Minister, who may have initiated further action, including discussing the incident with the Minister, Deputy Minister colleagues, the GCIO or other senior officials.

The entire course of events is illustrative of a series of missed opportunities and inaction, related to gaps in information, mistaken assumptions, limited knowledge, and insufficient awareness in related program areas.

5.0 Findings & Recommendations

The following is a summary of the findings of the internal review and based on those findings, recommendations for: 1) addressing the issues that led to the privacy breach; and, 2) improving government information security and management practices to prevent similar future incidences.

5.1. Incident Management and Investigations

Findings:

- Insufficient response and lack of effective communication, coordination and information sharing between employees, ministries and law enforcement*
- Ineffective review of, and response to, documents found at the employee's home.
 - Ineffective liaison with police to ensure applicable government offices were contacted and the appropriate level of information provided and shared.
 - Lack of personal initiative and follow-through to ensure the privacy breach was managed appropriately.

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

Action required:

- Create, within the Government's Chief Information Office (GCIO), an incident response team comprising security and privacy experts responsible for responding to, and managing information incidents.
- Review and streamline information incident policies and standards ensuring their effectiveness and implementation across government.
- Communicate and delineate information management processes and responsibilities for central agencies, ministries and programs including requirements to report immediately all information incidents to the GCIO.
- Create a law enforcement protocol for police and government to ensure, during the course of an investigation, effective information exchange and established internal and external communication practices.

5.2. Corporate Information Management

Findings:

Lack of knowledge of policies and practices regarding information privacy protection requirements

- Insufficient knowledge and understanding by employees, supervisors and managers regarding policies and requirements respecting personal and sensitive information and records management.
- Inadequate understanding of how to identify a privacy breach and appropriate steps to take to mitigate it, manage its impacts and reduce potential harm and misuse of the information.

Lack of clear policy direction regarding information management and security practices for employees

- Insufficient policy direction for employees, supervisors and managers related to the handling and security of government information for employees who periodically work off-site.
- Lack of clear policy direction regarding management of employees under investigation with respect to the use of, and access to, government information and systems.

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

Action required:

- Incorporate government information management policy and practice into new employee orientation and supervisor and manager training offered by the BCPSA and provide continuous learning opportunities for existing employees.
- Create greater employee awareness of information management practices through articles on government's key intranet sites such as @Work and @Your Service.

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

Action required:

- Revise human resource policies to ensure, where a human resource investigation reveals the involvement of government information and government information management systems, there is consultation with the GCIO, and that the employee under investigation is subject to appropriate controls and restrictions with regard to accessing government information.

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*

Action required:

- Review and consolidate current corporate policies to provide comprehensive guidance to employees and their supervisors on how to handle and ensure the security of personal and sensitive information outside of the workplace.

5.3 Ministry Information Management

Findings:

Inadequate knowledge and application of information and privacy security practices

- Insufficient privacy and records management knowledge and practices.
- Inconsistency between corporate and ministry information management and security policies and practices.

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*

Action required:

- Review and revise, with support from IAO, personal information management practices undertaken by the Medical Benefits Program.
- Ensure Medical Benefit Program employees are aware of their obligations for protecting personal information and require periodic and ongoing training of Medical Benefits Program staff in privacy, security and records management practices.

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

Action required:

- Review and revise the PLMS Branch, MHSD, investigation practices and breach procedures to ensure they align with corporate policy and practice.

Appendix 1 - Terms of Reference

Appendix 2 – Detailed Listing of Documents Found

Appendix 3 – Program Areas Involved

Appendix 4 – Policy Overview

Appendix 1 - Terms of Reference

Review of Privacy Breach

**Involving the Ministry of Housing and Social Development and
the Ministry of Children and Family Development**

Terms of Reference

Author: Wendy Taylor / Jason Eamer-Goult
Creation Date: November 3, 2009
Last Updated: November 23, 2009
Document Number:
Version: V 5.0

Approvals:

TOR Sponsors

Kim Henderson
Deputy Minister
Ministry of Citizens' Services

Approved by KH

Signature

November 23, 2009

Date

Dave Nikolejsin
Government Chief Information
Officer

Approved by DN

Signature

November 23, 2009

Date

Table of Contents

Table of Contents.....	2
Reviews and Document Control.....	3
1.0 Overview.....	4
2.0 Background.....	7
3.0 Breach Review Objectives:.....	4
4.0 Scope.....	4
4.1 In Scope.....	4
4.2 Out of Scope.....	4
5.0 Major Deliverables.....	5
6.0 Approach.....	5
7.0 Target Audiences / Participants.....	5
8.0 Milestones and Timeline.....	6

Reviews and Document Control

Reviews

This document has been sent to the following for their review and comment.

Name	Position
Dave Nikolejsin	GCIO
Kim Henderson	Deputy Minister, Ministry of Citizens' Services
Wendy Taylor	Executive Director, KIS Branch
Cairine MacDonald	Deputy Minister, Ministry of Housing and Social Development
Lesley du Toit	Deputy Minister, Ministry of Children and Family Development

Document Control

Date	Author	Version	Change Reference
November 9, 2009	KH	2.0	Changes requested by Kim Henderson
November 17, 2009	JEG	3.0	Changes made and forwarded for approval
November 17, 2009	WT	4.0	Changes made and forwarded for approval

1.0 Overview

This document outlines the objectives, scope, approach and deliverables associated with a review of a privacy breach related to clients of the ministries of Housing and Social Development and Children and Family Development. Once the review is complete, a final report will be produced that includes a summary of the effectiveness of existing policies and procedures and recommended improvements, as well as broad recommendations that reflect lessons learned to aid in the prevention of similar occurrences.

2.0 Background

In April 2009, during the course of an unrelated investigation, the RCMP seized documents containing sensitive personal information related to clients of the ministries of Housing and Social Development and Children and Family Development. Due to the circumstances, the Ministry of Children and Family (CFD) documents were not categorized as a privacy breach; however, the Housing and Social Development (HSD) documents were, and HSD was notified of the breach in July 2009. However, it was not until October 2009, after events transpired and additional information was made available surrounding the criminal investigation, that it was realized the extent and severity of potential privacy implications for both ministries' clients.

3.0 Breach Review Objectives:

The objectives of this review are to:

- Ensure Government's privacy breach protocol is comprehensive and relevant related to this category of breach, including timeliness and responses to actual or potential breaches;
- Determine the circumstances that led to the privacy breach and any necessary remedial steps;
- Identify opportunities to improve government and ministries' information security, information access and file storage and management practices.

4.0 Scope

4.1 In Scope

- The circumstances of the privacy breach, how it was managed and steps taken to remediate the situation.
- Government's processes, policies, systems, training and practices associated with privacy matters.
- Associated information management issues including legislative, corporate, core policy, CFD/HSD privacy and security policy requirements and affiliated information systems.

4.2 Out of Scope

- Matters pertaining to the criminal investigation.
- Matters pertaining to the management of personnel.

5.0 Major Deliverables

A final report that includes:

- Summary of relevant legislative, corporate, core policy, and CFD/HSD privacy and security policy requirements as applicable;
- The information management processes and practices established at the government and CFD/HSD level for the protection of both personal information and government's information resources and adherence to them in this circumstance;
- Review of, and recommendations to enhance government-level information management file management policies and practices;
- Review of relevant government information systems, including identification of employee data access permissions and audit trails to monitor such access;
- Review of how the privacy breach and security incident were handled and steps taken by MCFD/HSD to remediate the situation;
- Review and recommended changes in process, policy, systems, protocols, training and practices, if necessary, to reduce the possibility of such a breach occurring in the future; and
- Proposals for short-term solutions and long-term remedial approaches to address the implications of the breach and issues identified by this review.

Approach

The approach may include:

- a) Gathering documentary evidence;
- b) Surveying legislation, policies, practices, systems protocol;
- c) Meetings and interviews with involved parties and government officials; and
- d) Ongoing liaison with affected parties once the review is complete and the report released.

Target Audiences / Participants

Ministries of Citizens' Services, Housing, Social Development and Children and Family Development, Health Services (Ministry of Health Services may have relevant historical information).

Milestones and Timeline

<i>Milestone</i>	<i>Start Date</i>	<i>Target Date</i>
Gathering documentary evidence and survey of legislation, policies, etc.	November 23, 2009	December 4, 2009
Meetings or interviews completed	December 4, 2009	December 21, 2009
Draft report completed	January 4, 2009	January 15, 2010
Draft report circulated to affected parties and feedback received	January 18, 2009	January 25, 2010
Report finalized		January 29, 2010
Liaison with affected parties to ensure steps are commenced to implement recommendations	Ongoing	January 31, 2010

Appendix 2 – Detailed Listing of Documents Found

The following documents were retrieved from the employee's home:

- Eight "Caseload Management Reports", dated December 2006 to April 2007, for the Victoria Persons with Disability Employment and Assistance Office 107. Each report is 42 to 45 pages long and is identified with an office number, a worker number and a run date. There are about eight rows per page of the report, each listing a client and including names, birthdates, social insurance numbers, personal health numbers, GAIN file numbers, addresses, phone numbers, and cheque amounts issued to clients. Some of these clients are listed in more than one report;
- Three cheque signal reports dated Dec 15, 2006, Feb 16, 2007 and March 23, 2007, one page each, including clients' names and GA file numbers;
- Two copies of a one page CPP Income Load Case Review List, April 2007 including two clients' names and GA file numbers;
- One page Hardship and Transition Monitoring by worker report, March 23, 2007, including two clients' names, their social insurance numbers and GA file numbers;
- One page Financial Worker Field Advice report, March 23, 2007, including surnames and file numbers;
- One page Financial Worker Review Report, March 23, 2007 including surnames and file numbers;
- Two page Direct Cheque Register, March 23, 2007, including client and payee names, cheque amounts, and file numbers;
- 19 page blank template of a Ministry of Employment and Income Assistance Request for Proposals (RFP) number 46100AOB001 – Administered Assistance Services – Third Party application – issue date March 29, 2007; and,
- 30 MCFD printouts relating to 22 clients, including name, address, telephone number, birth date, gender, social insurance number, personal health number, client number, and listings of files opened with opened and closed dates.

Appendix 3: Program Areas Involved

MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT (MCFD)

The Ministry of Children and Family Development has approximately 4,500 FTEs (full time equivalents) and a budget of over \$1.3 billion. This large ministry delivers a diverse range of services, including child protection, youth justice, adoptions, child care, early childhood development and child and youth mental health. Three of its many branches were involved in this case.

Provincial Children and Youth with Special Needs Operations (PCYSNO)

There are four components to this branch. One of these is the Medical Benefits program, which funds medical equipment and supplies for severely handicapped children, as well as optical and medical benefits for children in care. The employee in question supervised one of two sub-units within the Medical Benefits component. Staff members in this unit do not work directly with children but, in the course of approving and processing payments, they require access to personal information about clients, including names, dates of birth, addresses, provincial health numbers and social insurance numbers. The two supervisors, who are union members, report to a manager excluded from union membership, who reports to a senior director responsible for the entire PCYSNO branch. This person, in turn, reported to an Assistant Deputy Minister responsible for Provincial Services (as part of a larger organizational change, PCYSNO now reports to a different ADM).

Strategic Human Resources (Strategic HR)

Human resource work within the public service is generally divided into two categories. The first comprises transactional and employee relations support to staff and managers for such matters as hiring, promotion, attendance management, discipline, and grievances. In most parts of government, this support is provided by the BCPSA. The second category is strategic human resources, which is concerned with workforce planning, employee engagement and organizational development. Strategic HR offices are located in each ministry. In most instances, ministry staff who work in Strategic HR do not deal with specific employees, but with the workforce as a whole. MCFD was unique within government in that, during the time of these events, Strategic HR was still dealing with some employee relations issues.

Ministry Chief Information Officer (MCIO)

Each ministry has a Ministry Chief Information Officer who is responsible for information management and information technology within the ministry, including records management, security, electronic service delivery and operational initiatives that are specific to the ministry. The Ministry Chief Information Officers (MCIOs) sit on the Government Chief Information Officers' Council to address cross-government policy and planning (see Government Chief Information Officer below). Employed within the MCIO's office was the Ministry Information Security Officer, who played an active role in this case.

MINISTRY OF CITIZENS' SERVICES (MCS)

The Ministry of Citizens' Services manages one of the most diverse portfolios in government, including the BC Public Service Agency, the Public Affairs Bureau, Enquiry BC, BC Bid, BC Stats, the Office of the Government Chief Information Officer, and Shared Services BC, which supports other parts of government by processing information requests, and supplying accommodation and technology. Three of its components were involved in this case.

BC Public Service Agency (BCPSA)

The Agency was formed in 2003 and is a "shared service" which provides human resource services to all parts of government. Although housed in MCS, it is accountable to the Province's Deputy Ministers' Council. The agency has a range of human resources expertise, but most of its work is "transactional" in nature: providing support to staff and managers in ministries for classification of positions, recruitment, promotion, performance management, employee illness and injuries, discipline and grievances.

Government Chief Information Officer (GCIO)

The Government Chief Information Officer (GCIO) is the governance authority for standards, oversight and approvals for the Province's information and communications technology. As government's chief information and technology strategist, the GCIO is responsible for promoting and guiding the effective management of government information. The GCIO is responsible for government-wide policy, procedures and standards related to data access, privacy, records management, security and electronic service delivery. The GCIO also leads strategic planning for information management and technology and develops mechanisms to ensure compliance with government-wide policies.

Information Access Operations, Shared Services BC (IAO)

IAO is the operational arm of government, which fulfills obligations under the *Freedom of Information and Protection of Privacy Act* and the *Document Disposal Act*. When citizens request information under the *FOIPPA*, staff in this office process the request. Previously, each ministry in government had its own information and privacy section. During 2009, they were brought together in IAO.

MINISTRY OF FINANCE

This Ministry has about 800 FTEs and a budget of approximately \$90 million. One small unit within the ministry was involved in these events.

Government Security Office (GSO)

This office was created in 1995 and is located in the Risk Management Branch. It seeks to reduce opportunities for harm to the people, assets and operations of government. It is one component of a larger "enterprise risk management" discipline, which identifies and mitigates risks across government. They promote harmonized policies and programs for security; provide advice and consultation; and broker information on successful risk mitigation. The two staff members are appointed as special constables, and have experience in policing, military service, intelligence, loss prevention and security.

MINISTRY OF HOUSING AND SOCIAL DEVELOPMENT (MHSD)

The Ministry of Housing and Social Development is a large, multi-faceted ministry created in 2008 to deliver employment and income assistance services, housing and homelessness strategies, labour market services, gaming policy and enforcement, and liquor control and licensing. It has approximately 2,600 employees and a budget of \$2.7 billion. Two of the Ministry's components were involved in this case.

Employment and Assistance program

This component, largely inherited from the former MEIA, helps people move from income assistance to sustainable employment, and provides income assistance to people unable to fully participate in the workforce. Employment and Assistance Workers meet directly with clients to determine their eligibility for services, authorize payments, and direct them to employment and other services, which will enable them to lead more independent lives. These services are provided in the Regional Services Division of the ministry. The employee in question in this review was employed from 2006 to 2007 as an Employment and Assistance Worker, and acquired most of the documents found in his home during this time.

Prevention and Loss Management Services (PLMS)

This branch is also located in the Regional Services Division of the MHSD, and is responsible for program integrity and loss management throughout the ministry. Their work is largely concerned with overpayments, and fraud allegations against those in receipt of ministry benefits. Ministry investigators also conduct certain internal investigations. About 20 investigators are designated special constables, and have legislated authority to share information with police for law enforcement purposes.

Freedom of Information and Protection of Privacy Act

- “[Personal information](#)” is “recorded information about an identifiable individual other than contact information”. (“[Contact information](#)” is “information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual”.)
- [Section 30](#): “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.”
- [Section 30.4](#): “An employee, officer or director of a public body or an employee or associate of a service provider who has access, whether authorized or unauthorized, to personal information in the custody or control of a public body, must not disclose that information except as authorized under this Act.”
- [Section 30.5](#): “An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an [unauthorized disclosure of personal information](#) that is in the custody or under the control of the public body must immediately notify the head of the public body.” Under [section 66](#), the responsibility of the head of the public body to receive such reports may be delegated to others.
- [Section 74.1](#) says that a person who contravenes sections 30.4 or 30.5 commits an offence.

Public Service Oath Regulation

- As a member of the British Columbia Public Service, I, , [employee name] do solemnly swear/affirm [circle one] that I will ... 2 honour and faithfully abide by the Standards of Conduct for Public Service Employees, and 3 to the best of my ability, ... (b) safeguard confidential information, not divulging it unless I am either authorized to do so or required to do so by law, ...

Standards of Conduct

- “Confidential information, in any form, that employees receive through their employment must not be disclosed, released, or transmitted to anyone other than persons who are authorized to receive the information. Employees with care or control of personal or sensitive information, electronic media, or devices must handle and dispose of these appropriately. Employees who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing, releasing, or transmitting it.

The proper handling and protection of confidential information is applicable both within and outside of government and continues to apply after the employment relationship ends.

Confidential information that employees receive through their employment must not be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains. (See the Conflicts of Interest section of this policy statement for details.)”

[Core Policies and Procedures Manual \(CPPM\)](#)

- [Chapter 12.3.1](#) concerns the Appropriate Use of Government Resources and indicates: “All users of government’s information and technology resources must take responsibility for, and accept the duty to, actively protect information and technology assets. This includes taking responsibility to be aware of, and adhere to, all relevant legislation, policies and standards.”
- [Chapter 20](#) covers Loss Management. When there is an information security incident that compromises protection of data or documents, the [procedure](#) for Chapter 20.2 requires that it be reported immediately to the GCIO and that a General Incident or Loss Report be provided to (amongst others) the ministry security officer and the deputy minister.

[Freedom of Information and Protection of Privacy Policy and Procedures Manual](#)

The Manual indicates, at section 30:

“Public bodies must:

- ensure their employees are trained to follow proper security procedures;
- monitor their employees’ compliance with security standards;
- ensure physical and procedural security precautions are established and maintained at appropriate levels; and,
- comply with the Core Policy and Procedures Manual’s security access matrix for recorded information.”

[Information Security Policy](#)

Chapter 7.7.2 of the [Information Security Policy](#) deals with information custodians’ responsibilities for mobile computing and “teleworking” (which includes employees working away from workplaces). Ministries are required to develop and publish policy for *ad hoc* teleworking (i.e., occasional telework), in particular the practice of removing material from the workplace.

The [Information Security Policy](#) also addresses “security incident” management. Chapter 9.2.1 requires ministries to establish a process for reporting, managing, responding to and recovering from information security incidents (which include breaches of confidentiality or privacy). Chapter 9.1.1 indicates that the

designated Ministry point of contact must report information security incidents to the Risk Management Branch using the General Incident and Loss Report, and to the GCIO. Chapter 9.2.1 says that when criminal activity is suspected, the Government Chief Information Officer and the Risk Management Branch must be consulted before the investigating officer contacts law enforcement agencies.

Chapter 4.2 of the [Information Security Policy](#) addresses Human Resources Security during employment. It indicates that managers must support the implementation of information security policies and practices by ensuring personnel are informed of information security roles and responsibilities. It also requires managers to provide ongoing information security awareness, education and training, addressing topics including on the protection of information.

Policy summaries

- [Working from Home](#)
- [Information Security Events and Incidents](#)
- [Human Resource Security](#).

Privacy breach policies

Both MCFD and HSD have processes for dealing with privacy breaches:

- MCFD has the *Privacy Breach Management Guidelines for Field Staff (July 2007)* and the procedure *Inappropriate Disclosure of Personal Information*;
- HSD has the *Guidelines for Handling a Privacy Breach*, *IPRS Internal Procedure for Completing a Privacy Breach Report*, *Questions and Answers for Breaches of Privacy*, and *Breach Protocols for Region 1 (updated December 2009)*.

At the time the RCMP removed the records from the employee's home, ministries were also able to access the GCIO's former *Guidelines for Handling a Privacy Breach*. These guidelines were replaced on October 30, 2009 with the more comprehensive [Policy and Procedure for Public Bodies Responding to Privacy Breaches](#). According to this new policy, a "privacy breach" is "a collection of, use of, disclosure of, access to, disposal of, or storage of personal information, whether accidental or deliberate, that is not authorized by the *FOIPP Act*."