Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F13-02

MINISTRY OF HEALTH

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

JUNE 26, 2013

CanLII Cite: 2013 BCIPC No. 14
Quicklaw Cite: [2013] B.C.I.P.C.D. No. 14

TABLE OF CONTENTS

Commissioner's Message:

Personal health information is much more than 'just data' – it is sensitive information provided confidentially in the context of care. The Ministry of Health ("Ministry") has custody of a large volume and wide range of health data about every British Columbian who receives publicly-funded health care, from such sources as the Medical Services Plan, PharmaNet, hospitals and mental health and addictions services.

This data is invaluable to health researchers seeking new solutions for patients and improved health outcomes for citizens. BC is fortunate to have a strong and vibrant community of researchers who are developing and testing new health treatments, and pioneering innovative drug therapies that are saving lives. These innovations have their roots in timely and secure access to health data.

It is therefore in the public interest for there to be active and effective research within the Ministry, health authorities and post-secondary institutions. However, the public, whose data it is, expects this research to be conducted responsibly and that their personal health data is managed securely in the research process.

This investigation examined three breaches of personal health data for research purposes that happened because the Ministry failed to translate privacy and security policies into meaningful business practices. The primary deficiency at the Ministry was a lack of effective governance, management and controls over access to personal health information.

At the time the breaches occurred, there was a lack of clear responsibility for privacy within the Ministry. This was due, in part I believe, to a lack of clarity of roles and responsibilities following the centralization of some information access and privacy functions. Ministry privacy governance was further weakened by a complete lack of audit and review of employee and contractor functions relating to privacy. There were no mechanisms to ensure that researchers were complying with the privacy requirements, as stipulated in contracts and written agreements, and to ensure that Ministry employees were taking appropriate privacy training and following privacy policies.

As a result, Ministry employees were able to download large amounts of personal health data onto unencrypted flash drives and share it with unauthorized persons, undetected.

These breaches indicate that the Ministry needs to establish clear leadership, responsibility and accountability for the proactive management of personal health information. The Ministry must establish control over personal health databases by developing an inventory that can be updated regularly. The Ministry needs to address gaps in privacy policies and provide adequate privacy training to all employees. The Ministry must audit and review privacy compliance by its employees and external researchers.

At the operational level, the Ministry should ensure that access to personal health data is restricted to employees who have a clear operational need. There should be technical safeguards in place to prevent employees from unauthorized copying or transferring that data from their workstations. In cases where transfer of data is authorized, employees should not use portable storage devices, except as a last resort. Even in those circumstances, such devices must be encrypted.

Many of the issues relating to research would be resolved, if all researchers, whether based in the Ministry, health authorities or post-secondary institutions, obtained access to personal health data only through a secure research environment, such as PopData BC. It is important that the Ministry review and adjudicate research requests in a timely manner and, should they be approved, provide access through the secure environment efficiently and without delay.

I note in the report that during the course of this investigation, the Ministry has implemented a number of significant improvements with respect to governance, policy development and physical security measures. Most importantly, it is moving towards the establishment of a highly secure environment for health research that uses personal health information.

The recommendations I have made in this report are essential to both facilitate access to information for health research in a more timely and secure manner and to address the privacy deficiencies identified by this investigation. Privacy and research are allies, not adversaries, in the pursuit of better health outcomes.

In tandem with this report, I am releasing a privacy management guide for public bodies entitled *Accountable Privacy Management in BC's Public Sector*. This new guide provides general information to assist public bodies with the design, implementation and maintenance of a privacy management program that suits the circumstances of the public body. The recommendations in this report reflect the principles of the guide tailored to the circumstances of the Ministry of Health.

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Executive Summary

This report provides an independent assessment of the privacy concerns arising from three disclosures of personal information that the Ministry brought to my attention in the context of a larger Ministry investigation into alleged conflicts of interest and contracting and hiring issues relating to research involving personal health information, which as of June 2013 was still ongoing. The Ministry accepts the three disclosures were unauthorized under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The report does not address criminal or civil culpability on the part of the Ministry, its employees or contractors.

In May 2012, the Ministry initiated an investigation of allegations related to contracting irregularities and inappropriate grant processes within its Pharmaceutical Services Division. Investigators discovered evidence that in another Ministry division there had been disclosures of personally identifiable health information that the Ministry believed contravened FIPPA ("alleged breaches"). While the information did not include names, it did include Personal Health Numbers ("PHN")[1] and other demographic information that could identify the subjects of the information with the sensitive health information contained in the disclosed information. The purported recipients of the information were two contractors and a researcher. The Ministry informed this Office of the alleged breaches.

This Office's investigation confirmed that the three disclosures were unauthorized. The investigation also reviewed the response of the Ministry to these breaches to determine whether the Ministry was meeting the requirement of section 30 of FIPPA to provide adequate security to prevent the unauthorized access, use or disclosure of personal information.

The disclosures of personally identifiable information occurred because it was possible for employees with access to Ministry databases to copy personally identifiable information onto unencrypted flash drives without an audit log or other security measures detecting this access or disclosure.

The investigation found deficiencies in the Ministry's privacy and security safeguards for personal information. Ministry databases containing personally identifiable information did not have sufficient technological controls over access, use and disclosure of personal information. The Ministry also did not monitor or audit compliance with privacy policies or privacy provisions in agreements. The

[1] The PHN is a unique identifier that is assigned to every British Columbian enrolled in the provincial Medical Services Plan.

lack of internal controls was illustrated by the fact that the Ministry did not discover the unauthorized disclosures until it conducted a detailed examination of thousands of emails and files on hard drives of several employees, after advice from a whistleblower.

The Ministry failed to protect privacy appropriately in contracts with some service providers. In addition, it is not maintaining a record of personal information databases as required by FIPPA.

The Ministry's immediate response to the unauthorized disclosures was adequate. However, the deficiencies in the Ministry's controls over personal information mean the Ministry was not providing adequate security to prevent unauthorized disclosure of personal information at the time of these disclosures. This is a contravention of s. 30 of FIPPA.

Implementing a privacy and security risk management program is essential to enable the Ministry to address these and other deficiencies outlined in this report.

I am deeply concerned that, 20 years after the introduction of FIPPA, the Ministry's approach to privacy and security management for the personal information in its custody and control would contain such deficiencies. The public expects there to be adequate safeguards to protect personal information, both in the delivery of health care and research using health data. Advances in information technology necessitate a much more comprehensive approach to privacy and security risk management than ever before. Helpfully, there are many local examples of model compliance practices available for the Ministry to adopt.

I encourage all public bodies and organizations that manage personal information to make use of the resources available for privacy management. Tools and guidance to ensure an effective privacy management program are available on our website.[2] Another useful tool for public bodies particularly involved in health research is the Canadian Institutes of Health Research's "Best Practices for Protecting Privacy in Health Research (September 2005)".[3] By following this guidance, the Ministry, health authorities and post-secondary research institutions can promote important health research while protecting the privacy of patients whose information is under study.

[2] These are available on the Office website at http://www.oipc.bc.ca/tools-guidance/guidance-documents.aspx.
[3] http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf.

1.0 PURPOSE AND SCOPE OF THE REPORT

1.1 Introduction

This investigation is authorized under s. 42(1)(a) of FIPPA, which grants this Office the authority to conduct investigations to ensure compliance with any provision of the legislation.

The purpose of this investigation was:

- to determine whether three disclosures of personal information contravened FIPPA; and
- to determine whether the Ministry had implemented reasonable security arrangements to protect the personal information at issue against unauthorized access, use or disclosure.

The investigation examined the disclosures, and identified a number of deficiencies with respect to security of personal health information in Ministry databases. These deficiencies require the Ministry to improve its privacy management to reduce the risk of future unauthorized disclosures.

1.2 Background

In March 2012, the Office of the Auditor General of BC advised the Ministry of a complaint alleging irregular contracting and research practices, including inappropriate access to personal information in the Research and Evidence Development section of the Pharmaceutical Services Division of the Ministry. The Ministry initiated an investigation and the Office of the Chief Information Officer (“OCIO”) assigned a privacy investigator to lead the investigation.

On July 13, 2012, the Ministry informed this Office that it was conducting an investigation that might uncover suspected unauthorized disclosures of personally identifiable health information. The Ministry remained in regular contact with this Office on the progress of its investigation and provided this Office access to copies of relevant records.

On September 10, 2012, the Ministry notified this Office that it had found evidence that an employee had provided a contracted service provider with access to personal information contrary to s. 33 of FIPPA.

On September 11, 2012, this Office notified the Ministry that it was formally investigating this disclosure. The scope of the investigation was to assess the nature and extent of the disclosure, whether it contravened s. 33 of FIPPA and whether the Ministry was complying with the security requirements of s. 30 of FIPPA. The investigation also reviewed whether this disclosure of personal information for research purposes complied with the requirements of s. 35 or was otherwise authorized under FIPPA.

Further investigation by the Ministry and this Office revealed that there were two other instances where an employee disclosed personal information without authorization. These two disclosures also formed part of this investigation.

The Ministry discloses personal health data for Ministry research purposes and to external researchers for their own academic research purposes. With respect to Ministry research purposes, in some cases, Ministry employees conduct the research. In other cases, the Ministry contracts with external researchers to conduct research at the direction of the Ministry ("contracted researcher"). The Ministry also discloses personal health data to support independent academic research for approved research proposals ("academic researcher"). At the time our investigation began, there were four processes for disclosure of Ministry data. Most applications were received by the Office of the Chief Data Steward and the Information Management and Knowledge Services branch. Applications were approved by the Information Management and Knowledge Services branch or by the Data Stewardship Committee, an arm's length body appointed by the Minister. The approved process for Ministry employees and contracted researchers involved Data Access Services staff in the Ministry coordinating the delivery of the data through the Health*Ideas* data warehouse and various legacy systems in a manner that was direct, secure and authenticated.

1.3 The Disclosure of Personal Information at Issue

This investigation examined three disclosures of personal information. These three cases are the only ones that had come to light at the time this report was issued. As the Ministry continues to investigate these matters, it is possible that there could be more.

The first case involved the disclosure of personal health information by an employee to a contracted service provider[4] in June 2012.

[4] Under FIPPA, a contracted service provider is considered to be the same as an employee of a public body and subject to the same privacy obligations as an employee. When one employee shares personal information with another employee of the same public body, the disclosure must be authorized by FIPPA.

On May 31, 2012, the contractor asked a Ministry employee for a table that had two years of health information for each of the approximately 4 million people in the province, which combined represented 8 million rows of information. The information was needed for testing purposes. Each row represented an individual, and was to have up to 19 fields of health information. The fields included PHNs; number of mental health service encounters; whether the individual had diabetes; number and length of hospital stays; and all services billed for the person.

The contractor requested that the PHNs be masked or removed, as the testing process did not need such sensitive personal information. On June 6, 2012, the employee provided the contractor with the requested information on a portable storage device. On June 8, 2012, the contractor noticed that the information file contained unencrypted PHNs.[5] The contractor immediately deleted the PHNs from his work computer and returned the flash drive to the Ministry employee.

The second case involved the disclosure of personal health information to a contracted researcher. On October 4, 2010, the researcher contracted with the Ministry to conduct data analysis. The contracted researcher subsequently submitted a request to the Ministry, under established Ministry procedures, for access to the information necessary to conduct the analysis. The employee gave the contracted researcher a portable storage device with health information of over 20,000 individuals including PHNs, ages and information gathered from chronic disease registries including diagnoses and pharmaceutical histories.

However, according to the Ministry, the employee, who had access to the data for his Ministry work, was not authorized to disclose data to other employees, contracted researchers or academic researchers. Ministry procedures for access to health data for research involve researchers receiving data though an approved and secure process. The device was also unencrypted, contrary to the repeated advice on this matter from this Office, provided in a series of recent Investigation Reports.[6]

The third case involved the disclosure in June 2012 of Canadian Community Health Survey ("CCHS") information. In the autumn of 2011, another employee who was also an academic researcher, requested personal health information. The personal information included Medical Services Plan billing records, hospital discharge summaries, PharmaCare prescriptions and information gathered by Statistics Canada under the CCHS.

[5] It is not clear why the employee included unencrypted PHNs.

[6] University of Victoria, F12-02, 2012 BCIPC 7 (CanLII); Vancouver Coastal Health Authority, F06-02, 2006 CanLII 20511; and the Ministry of Labour and Citizens' Services (as it then was), F06-01, 2006 CanLII 13536.

The CCHS survey collects a large volume of sensitive personal health information on the basis of consent and strict conditions for data use, collection and disclosure. There are approximately 50 categories of questions, including questions about alcohol use, drug use, mental health, self-esteem and sexual health. The survey results also include individual's PHN, age, birth date, gender and full postal code.

Statistics Canada shares CCHS survey results with the Ministry under a signed agreement that the Ministry not disclose any of the information in personally identifiable form to parties outside of the Ministry. Statistics Canada had promised individuals who completed the survey that the Ministry would not disclose any of their information in personally identifiable form.

On June 28, 2012, the employee gave the other employee a portable storage device with all of the requested personal information. According to the Ministry, as in the previous case, the employee was not authorized to disclose data to this individual.

2.0 ISSUES

The question for this Office is whether the Ministry had reasonable security arrangements in place to protect personal health information from unauthorized access or disclosure, as required under s. 30 of FIPPA.

2.1 Preliminary Issues

The BC Ministry of Health, as a ministry of the government of British Columbia, falls within the definition of a "public body", and therefore is required to comply with FIPPA. FIPPA prohibits the disclosure of personal information by public bodies, except where it is authorized in accordance with s. 33. One of the provisions of s. 33 of FIPPA permits disclosure of personal information for a research purpose without the consent of the individual, where the research is in accordance with s. 35 of FIPPA.

The Ministry acknowledges that the three disclosures involved personal information as defined by FIPPA. It also concluded that the disclosures were not in accordance with any provision of s. 33 of FIPPA, as the employee had no authority to disclosure the personal information. The Ministry also determined that s. 35 of FIPPA did not apply. As the Ministry takes the position that the disclosures contravened s. 33 of FIPPA, there is no need to make a formal finding. I note that, while the Ministry might have been authorized to disclose the personal information to the contracted researcher and employee through an approved process, I am satisfied that FIPPA did not authorize the particular employee involved to disclose this information.

Did the Ministry have reasonable security arrangements in place to protect personal health information from unauthorized access, use or disclosure, as required under s. 30 of FIPPA?

In addressing this question, the investigation examined the general security arrangements in place prior to the occurrence of the breaches and the Ministry's response to the breaches.

General security arrangements at the time of the breaches

Section 30 of FIPPA requires public bodies to make reasonable security arrangements to protect personal information in their custody or under their control. Section 30 states:

> **Protection of personal information**
>
> 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.

The reasonableness standard in s. 30 is measured on an objective basis and, while it does not require perfection, depending on the situation, it may signify a high level of rigor. To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards.

The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, the estimated costs of security, the relationship between the public body and the affected individuals and how valuable the information might be for someone intending to misuse it.[7]

The disclosures of personal information in the three cases cited above occurred because an employee was not detected as they accessed databases and copied personal information onto unencrypted flash drives. In the process of investigating the circumstances that made these disclosures possible, the investigation identified a number of weaknesses in Ministry controls over personal information.

[7] University of Victoria, F12-02, 2012 BCIPC 7 (CanLII).

Portable storage devices

Unencrypted portable storage devices were used in all three disclosures. Government-wide policy on use of portable storage devices states that they must be encrypted.

Storing personally identifiable information on portable storage devices involves an unacceptable and unreasonable level of risk of misuse of the information. This Office has investigated a large number of privacy breaches involving the loss of laptop computers, flash drives and CD-ROMs containing personal information. There are innumerable media reports of similar losses across Canada and internationally.

Encryption helps to mitigate the risk, but is not always a complete solution. Public bodies and private sector organizations need to explore alternative secure methods of remote access to personally identifiable information, and resort only to encrypted portable devices when all other, more secure, options are not available.

A more secure practice to disclose information for research is to utilize a secure research environment containing technical safeguards that prevent the transfer of information to portable storage devices. This could include disclosure through a secure internet site, or by providing direct, tailored and time limited access to the relevant databases. One example of how to facilitate access to health information for research in a secure environment is PopData BC.[8]

RECOMMENDATION 1:

The Ministry should develop and implement additions to the BC Government policy on the use of portable storage devices to require the use of other, more secure, forms of information transfer. Portable storage devices should only be used as a last resort and must always be encrypted.

Access controls for employees

A necessary requirement of providing adequate security for personal information on electronic systems is appropriate and effective user access controls. The foundational principle of information access in Ministry and government policies

[8] http://www.popdata.bc.ca.

is “least privilege” or “need to know”, which are defined in Chapter 12 of the Province’s Core Policy and Procedures Manual, as follows:

> *Need-to-Know*
>
> A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office.
>
> The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on all information systems.
>
> *Least Privilege*
>
> A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Chapter 7 of the OCIO’s Information Security Policy identifies best practices and responsibilities for creating access controls to restrict access to government information. In particular, access policies must include the following:

> **7.1.1 a) Access control policy**
>
> *Information Owners* and *Information Custodians* are responsible for establishing, documenting and approving access control policies which must:
>
> - Support and enable business requirements identified in *Privacy Impact Assessments*;
> - Be based upon *Security Threat and Risk Assessments*; and
> - Include classification of *assets*.
>
> Access control policies must additionally:
>
> - Consider both physical and logical access to assets;
> - Apply the “*need to know*” and “*least privilege*” principles;
> - Set default access privileges to “deny-all” prior to granting access;
> - Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable;
> - Have permissions assigned to roles rather than individual user identifiers.

Government policy and privacy and security best practices also require that the access control policy must be communicated to personnel as part of awareness training.[9]

The investigation found that current access privilege systems at the Ministry of Health do not consistently comply with the principles or controls set out above. The Ministry does not assign permissions to roles, which is the best practice. Access permissions are assigned to business groups within the Ministry and the level of permissions assigned to an individual is based on the type of group an individual belongs to. Individuals are then assigned to one of these groups. Permissions are not necessarily removed when an employee's roles change.

The Health Information Privacy, Security and Legislation branch in the Ministry has recognized this problem and supports the implementation of a role-based access model for all employees and a reliable process for adjusting access levels for employees when their job functions change.[10]

The Ministry has acknowledged that some employees have access to levels of information beyond what they require for their jobs. Even in cases of Ministry employees who had legitimate reasons for access to a broad range of Ministry information, their ability to access, use and disclose the information and to copy it to portable storage devices, unmonitored by an access log, was contrary to the least privilege principle.

In simple terms, such employees had excessive access to personal information with inadequate tools in place to manage the risk such wide access poses.

The Ministry also has difficulty ensuring that there are appropriate controls on all of its databases because Ministry employees are able to copy and store personal information from databases to other locations including personal storage devices or personal hard drives within the Ministry.

The Ministry should be able to control, track and audit employee-access privileges to all databases and ensure that they comply with the need to know and least privilege principles. It should also implement security measures to make unauthorized transfer of personal information from databases technically impossible.

[9] Information Security Policy (p. 98), Version 2.2, October 2012, Office of the Government Chief Information Officer, Ministry of Citizens' Services and Open Government.

[10] See below p. 26 for a discussion of the role of this branch.

RECOMMENDATION 2:

The Ministry should ensure user privileges are granted and managed based on the need to know and least privilege principles, ensuring that employees have access only to the minimum amount of personal information they require to perform their employment duties. Access permissions should be assigned consistently and kept up to date.

RECOMMENDATION 3:

The Ministry should implement technical security measures to prevent unauthorized transfer of personal information from databases.

Monitoring access, use and disclosure

Further heightening the risks of unauthorized access, use and disclosure of personal information in the Ministry was a complete lack of monitoring, enforcement and evaluation. There was no audit at any level of employee or researcher compliance with privacy policies. Nor did the Ministry conduct any reviews of privacy provisions in agreements that provide for information sharing.

Government policy gives the Office of the Chief Information Officer the authority to develop privacy policies and standards for ministries and evaluate their compliance.[11] The Health Information Privacy, Security and Legislation branch and the Information Management and Knowledge Services branch in the Ministry have responsibility for monitoring compliance by the Ministry with those policies and standards. Representatives from all three told us that they lacked the resources to undertake effective evaluation or monitoring of compliance. This response, given the large volume of personal information in the Ministry is unacceptable; it indicates a lack of sufficient executive commitment, on the part of the Ministry and government corporately, to privacy and security compliance.

The current information management infrastructure at the Ministry presents particular challenges to proper monitoring and compliance with privacy policies. Legacy databases lack easy methods to proactively detect and investigate

[11] Core Policy and Procedures Manual, Chapter 12.2.2, IM/IT Governance, available at: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm.

unauthorized access and removal of information. It appears that most of the databases lack the ability to trace employee access to information.

These problems became evident when the Ministry tried to investigate the extent of the potential privacy breaches, after the whistleblower identified the issue. None of the systems flagged or otherwise indicated any evidence of a breach. The Ministry was only able to determine the details of the actual breaches through a laborious review of the employees email and personal computer hard drives, as no other auditing trail was able to detect the privacy breaches before or after their occurrence.

None of the Ministry's privacy or security controls detected or recorded in an activity log any of the unauthorized disclosures. In fact, even after the Ministry suspended information access for certain Ministry contracted researchers and employees, they were still able to access and disclose the information involved in the breaches at issue in this report. Some employees told academic researchers that they could access information for them, despite the suspension of those researchers' access privileges.

In attempting to contain the breaches, the Ministry had to rely on declarations from the employees and contracted researchers under investigation that they did not have any Ministry information stored outside the confines of the Ministry. The limited ability to detect unauthorized access to and activity on Ministry databases can slow the containment of breaches, because, as the Ministry experienced, it is time consuming to obtain any evidence about when or how much information is involved.

One particular problem of the absence of any monitoring is that the resources invested in ensuring thorough privacy protection within information sharing agreements might be wasted because there is no follow-up to ensure researchers are complying with privacy and security requirements.

It is essential to require periodic audits and reviews to ensure that employees, contracted researchers and academic researchers are complying with those policies. The Ministry also needs to audit whether contracted researchers with access to information are complying with the terms of their agreements, such as the one with Statistics Canada, which restrict access to certain categories of information.

Prior to signing information sharing agreements with research institutions or research agreements with individual academic researchers, the Ministry must ensure that they will have the ability to audit the activities of researchers to verify that they are complying with the terms of their agreements.

RECOMMENDATION 4

The Ministry executive should implement an effective program for monitoring and auditing compliance by employees with privacy controls, and by contracted researchers and academic researchers with privacy provisions in agreements, to enable proactive detection of unauthorized use and disclosure of Ministry information.

Until the Ministry establishes better controls over the number of databases containing personally identifiable health information dispersed throughout the organization, it will continue to be vulnerable to privacy breaches. Ultimately, the Ministry should work towards having a secure research environment in which all Ministry personal information resides, where access privileges can be tailored to individuals, and use and disclosure can be easily monitored, audited and controlled.

The Ministry has taken some steps to address the current weaknesses in security over personal information. One example is the Ministry's data warehouse project, Health*Ideas* BC, which provides the modern architecture to enable privacy and security to be effectively managed and monitored. The Ministry is increasing the amount of information that resides inside Health*Ideas* BC*.*

The Ministry is also increasingly utilizing a UBC-operated secure research environment, PopData BC, for information access requests from researchers outside the Ministry. PopData BC includes automated warnings when certain risky behaviours, such as downloads of large amounts of information are detected. It also has built-in safeguards, including using technology to detect and prevent access to information from a computer outside of Canada. These initiatives will help to improve overall privacy compliance in the Ministry.

Management of contracted researchers and academic researchers

The Ministry discloses personally identifiable information to contracted researchers through contracts and academic researchers through research agreements. This report already noted above the lack of monitoring of compliance with privacy provisions in these agreements. Another problem is that the privacy and security provisions of the contracts we reviewed varied greatly, with some falling significantly below an acceptable standard for protecting personal information.

Some Ministry contracts included information sharing agreements with specific privacy protection schedules. Other agreements, including the contract with one of the researchers involved in the privacy breach, used a standard government-wide agreement for services template to provide access to information, which in those cases did not incorporate sufficient privacy controls. In addition, some contracts referred to appendices regarding security controls, but those appendices did not exist. Other contracts did not include an oath of confidentiality or a specific confidentiality agreement. Although some contractors may be subject to general code of conduct agreements that cover some aspects of privacy, a specific confidentiality agreement provides a greater level of assurance.

Information Management and Knowledge Services branch is working with contract management staff in Ministry program areas to prevent general service agreements being used to circumvent proper privacy controls over access to information. This branch intends to educate contracted researchers and Ministry staff entering into contracts. Such contracts should include detailed privacy protection obligations. In cases where the Ministry is providing data in support of academic research, or where the agreement is otherwise strictly about information sharing, the Ministry should use an information sharing agreement, or research agreement, with detailed privacy obligations.

RECOMMENDATION 5:

The Ministry should ensure that all contracts with contracted researchers and research agreements with academic researchers involving the disclosure of personal health information provide for an appropriate level of security, including privacy protection schedules. These requirements should include limiting the use and disclosure of personal information to specified contractual purposes; taking reasonable security measures to protect personal information; requiring compliance with privacy policies and controls with respect to storage, retention and secure disposal; and requiring notice to the Ministry in the event of a privacy related contractual breach. The Ministry also should use information sharing agreements wherever the substance of an agreement is about information sharing, rather than the provision of services to the Ministry.

Personal information inventory

In order for a public body to provide adequate security for personal information in its databases, the public body must have a clear idea of where data is collected and stored. A thorough personal information inventory is a fundamental, critically important aspect of privacy compliance. At the time of our investigation, the Ministry did not possess a comprehensive inventory of where information resides within the Ministry. It would be beneficial for the Ministry to develop an inventory of personal information databases and data flows, with the objective of creating a regularly updated repository for the Ministry. There would be further benefits in periodically reviewing this inventory to identify those dataset extracts and other sensitive information assets that can be archived or deleted.

RECOMMENDATION 6:

The Ministry should develop a comprehensive inventory of all databases containing personal health information. The inventory should be updated regularly and should set out associated information flows relating to collection and disclosure for research purposes.

Finding One:

Personal health information is one of the most sensitive categories of personal information held by public bodies. This level of sensitivity requires an accordingly high level of physical, administrative and technical security measures. It is clear from this analysis that the Ministry did not have sufficient safeguards in place and that it did not allocate sufficient resources to protect personal information in its custody. The Ministry did not have an adequate inventory of databases or administer appropriate access controls on its employees.

There were insufficient physical and technological safeguards to prevent copying of sensitive personal information onto portable storage devices. The Ministry failed to monitor the access, use and disclosure of sensitive personal information. It also failed to impose effective security provisions in some of its contracts and information sharing agreements. Given the level of sensitivity of the personal information involved, the Ministry did not provide reasonable security.

Finding 1: **I find that, at the time of the unauthorized disclosures, the Ministry did not have reasonable security in place to protect personally identifiable information from unauthorized access or disclosure to the standard that s. 30 of FIPPA requires.**

2.2 The Ministry's Response to the Breaches

Investigation Report F11-03[12] stated:

> [A]ll public bodies and organizations need to exercise due diligence in protecting the security of personal information in their custody or under their control. Security of systems requires ongoing vigilance. Public bodies must respond quickly to any identified privacy and security risks. Failure to do so would certainly not meet the requirements of FIPPA.

A public body's obligations under s. 30 include the actions it takes when there has been a privacy breach. In an investigation into the sale of surplus government data tapes, former Commissioner Loukidelis outlined what a public body must do when responding to a privacy breach:

> In order to assist public bodies, the OIPC has published a key steps document for managing privacy breaches.[13] 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's key steps document has been useful in our review and evaluation of the Ministry's actions in this case. The four key steps public bodies must undertake in managing a privacy breach are:
>
> 1. Contain the breach;
> 2. Evaluate the risks;
> 3. Determine whether notification of affected individuals is required; and
> 4. Develop prevention strategies to reduce risks in the future.
>
> The first three steps should occur as soon as possible following the breach, either simultaneously or in quick succession.[14]

This assessment of the Ministry's response to the three disclosures is organized around these four key steps.

1. Breach Containment

When the Ministry uncovered evidence of unauthorized disclosures it followed the direction in the *Key Steps* and in the OCIO's *Process for Responding to Privacy Breaches*. It also notified this Office. The Ministry, unsure of the scope of the breach, attempted to contain potential unauthorized disclosures by suspending access to Ministry information by Ministry staff and external researchers. Some access was restored as the scope of the breach became

[12] 2011 BCIPC 43 CanLII.
[13] Privacy Breaches: Tools and Resources, http://www.oipc.bc.ca/guidance-documents/1428.
[14] Ministry of Health, F08-02, 2008 CanLII 21699.

clearer upon further investigation. The Ministry, conscious that it was difficult to determine the extent of the disclosures, continues to investigate (as at June 2013) and acknowledges that it is possible that there could yet be more unauthorized disclosures discovered.

Once the Ministry identified the three disclosures at issue in this report, it attempted to retrieve the information held outside the Ministry. The Ministry wrote letters to key individuals demanding that they securely return any Ministry owned data or information in their possession, including personal information. The Ministry also demanded that, if any of the information was disclosed to a third party, the individuals were required to inform the Ministry of the details of the disclosure. Finally, the Ministry demanded that the individuals sign written declarations that they did not possess Ministry data, including personal information, on any computer or storage device or did not possess similar records in written form. Eventually, all the individuals to whom the Ministry sent letters, either signed a declaration that they did not possess Ministry owned personal information or provided statements to that effect.

The Ministry also searched employee emails and the hard drives of employee computers for copies of the information. It is worth noting the high costs of such after-the-fact privacy breach management as opposed to investing in comprehensive privacy and security risk management up front. Senior management time is an especially high component of this burden.

Overall, the Ministry's immediate breach containment efforts were reasonable. The Ministry devoted considerable resources and several strategies to try to limit the further dissemination of the personal information at issue and to recover it from the researchers.

I conclude that the Ministry made reasonable efforts to contain the breaches in the circumstances.

2. Risk Evaluation

To determine what additional steps are required in response to a breach, public bodies are expected to evaluate the risks associated with the unauthorized disclosures. The Ministry produced a risk assessment after it had determined the extent of the disclosures, in order to guide its decision whether notification of individuals was appropriate. The Ministry determined that the personal information involved in the disclosures had been either deleted, returned or the recipients had signed documents saying they did not have any Ministry information.

The Ministry believed that information from two of the three disclosures was shared in a format that was only accessible with particular software and, therefore, posed minimal risk of further disclosure. However, our investigation determined that the software was commonly used and was easily available.

The Ministry also determined that there was no evidence that foreseeable harm could result from these disclosures. This was based on its assessment that there was no evidence that those who received the information had used, or would use, it inappropriately. The Ministry also noted that there was little risk of identity theft, physical harm or loss of business or employment. The Ministry believed the research credentials of the individuals involved suggested that there was little risk for misuse. In summary, the Ministry concluded there was no reason to conclude that the individuals involved had used, or would use, the information for other than the intended research purposes or to harm a third party.

While the Ministry's initial risk assessment considered many relevant factors, it did not consider all of them. A particular omission was that the assessment did not consider the sensitivity of the data. In concluding that there was a low likelihood of direct harm to affected individuals, the assessment overlooked the indirect harm of loss of assurance and public trust arising from the unauthorized disclosures, especially given media coverage of these breaches, staff terminations and the Ministry's broader investigation.

Overall, the Ministry's risk assessment was adequate in certain respects but was not complete. This led the Ministry initially to conclude that the breaches were not serious enough to warrant notification of the individuals whose information was at issue.

3. Notification

After consultation and deliberation with this Office, the Ministry decided to directly notify the affected participants in the CCHS survey and to make a general public notification with respect to the other two disclosures.

Direct notification for CCHS survey participants was desirable for two reasons. The first was that the Ministry had broken the commitment that Statistics Canada had made that none of its personally identifiable information would be disclosed. Another reason was because it is important to weigh the general harm to individuals and the breach of trust that arises from an unauthorized disclosure of personal information. This is the case even where evidence of direct harm from the unauthorized disclosure is low.

The Ministry convened a news conference on January 14, 2013, to inform the public of details of the breaches. It mailed letters of notification to affected individuals (approximately 37,000) in batches over five days starting on January 16, 2013. The Ministry made use of a website and a toll-free call centre to make additional information available to affected individuals.

The direct notifications to the CCHS survey participants consisted of a letter which contained:

- a description of the personal information that was disclosed;
- the results of the Ministry's investigation of the disclosures and its conclusion that they would not cause harm;
- a reference to this Office's investigation; and
- details of how affected individuals with questions could obtain further information.

One significant issue with respect to the notification was its timeliness. The Ministry was aware of the details of the alleged breaches in September 2012, but did not issue the notification for approximately four months. This was a lengthy delay in the circumstances.

Determining a reasonable timeline for notification depends on the circumstances of the case. Where there is risk of immediate harm, such as identity theft, there is a greater need to inform affected individuals quickly, so that they can take appropriate measures to protect their interests, such as change bank accounts. The privacy breach involving employee payroll information at the University of Victoria is an example where there was a pressing need to inform affected individuals, whose names and financial information had been stolen. In that case, the University of Victoria notified almost all the affected individuals the day after the breach was discovered.[15]

In this case, there was a low risk of the information being used for identity theft. The potential harm was that aspects of the affected individuals' medical history would become known. But there was no evidence that the contractors or researcher had further disseminated the information. The Ministry considered that the information recipients, as legitimate researchers, only intended to use the information for research purposes that would not involve identifying the participants. They saw no evidence of intent to use the information for any malicious purpose.

The Ministry indicated that it wanted to gather more information about the extent and risks of the disclosures before notification to avoid causing undue alarm to the affected individuals. As concern about direct harm to the individuals was low, there was not a pressing need to notify the participants immediately.

While I decline, with hindsight, to stipulate precise timelines during which the Ministry ought to have responded, a delay of four months was longer than desirable in this case. Even in cases where there is not a pressing need to notify

[15] University of Victoria F12-02, 2012 BCIPC 7 (CanLII) at para. 4.4.

and there are justifications for a modest delay, notification should happen as soon as it is feasible. Public bodies and organizations should not use this case as a standard for assessing notification in a reasonable time frame.

4. Prevention Strategies

Following discovery of the breaches, the Ministry took a number of initiatives to reduce the risk of further breaches in future, including:

- commissioning a private consulting firm to evaluate the Ministry's internal security controls over personal health information and to provide options for remediation of any control weaknesses;

- implementing a Data Research Policy to guide the Ministry on appropriate access to information for research; and

- improving its physical, technical and administrative security controls over CCHS survey information, to comply with security requirements required by Stats Canada.

Other initiatives underway that will help strengthen data protection in the Ministry are discussed elsewhere in this report. These efforts combined, address most of the information security issues that this report raised. Therefore, I find that the prevention strategies are reasonable.

Finding Two:

The Ministry's attempts to contain the breach, on balance, were reasonable in the circumstances. The Ministry's evaluation of the risk to affected individuals would have been stronger if it had considered the less tangible harms to affected individuals, most notably the breach of trust arising from the unauthorized disclosures.

Although it should have been timelier, the Ministry's process of notification was reasonable. The Ministry has already taken some steps to prevent similar breaches in future, and this report identifies several additional areas where actions are required to satisfy the requirements of s. 30.

Finding 2: I find that the Ministry's immediate response to the unauthorized disclosures was reasonable and met the requirements of s. 30 of FIPPA.

3.0 THE VALUE OF A PRIVACY MANAGEMENT PROGRAM

This case illustrates the value of a privacy management program that encompasses privacy and security risk assessment. While such a program is not a requirement for public bodies to comply with s. 30 of FIPPA, it is a best practice to assist public bodies with overall compliance and to minimize the risk of privacy breaches. In discussing the requirements of s. 30 in Investigation Report F11-03,[16] I stated:

> reasonableness extends beyond a measure of responsiveness to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their systems. Public bodies also must ensure their policies are kept current and that their staff receives regular training.

In short, good privacy management is critical to managing the risk of harm to citizens and to ensuring public trust. A privacy management program identifies and organizes all of the tasks a public body can undertake to meet its obligations to protect personal information. It is an invaluable tool to strengthen good privacy practices, identify weaknesses, demonstrate due diligence and develop privacy protection that rises above the minimum required by FIPPA. *Accountable Privacy Management in BC's Public Sector,*[17] is an outline of the elements of a robust privacy management program. I highlight below some of the Ministry's current privacy practices that could be improved as part of implementing an effective privacy management program.

Effective privacy governance

In its broadest sense, privacy governance over personal health information used for research within the Ministry is a complex web of different offices and officers, some of which reside outside of the Ministry. One reason for this complexity is that in 2009, the provincial government centralized information and privacy program functions, transferred some employees and realigned some of the responsibilities. Nevertheless, the Ministry still retains accountability for privacy compliance, which (after 2009) it has had to meet with diminished privacy resources.

The Core Manual outlines the redistribution of governance and accountability for privacy in basic general terms between the OCIO and Ministry CIOs.

However, there is no explicit documentation that indicates how specific responsibilities are divided between the OCIO and the Ministry.

[16] 2011 BCIPC 43 (CanLII).

[17] http://www.oipc.bc.ca/tools-guidance/guidance-documents.aspx. See *also Getting Accountability Right with a Privacy Management Program* http://www.oipc.bc.ca/guidance-documents/1435 for more information about privacy management programs.

A key component of good privacy governance is a clear accountability policy that designates who is responsible for the various aspects of the privacy management program. Greater clarity about the respective roles and responsibilities of the Minister, the OCIO, the MCIOs, and other branches of the Ministry helps all employees to do their part in ensuring effective privacy management.

The role of the Health Information Privacy Security and Legislation branch has also been recently expanded, to provide a greater profile to privacy and security generally in the Ministry. This branch previously had a narrow mandate which meant it was not responsible for championing privacy within the Ministry.

Health Information Privacy Security and Legislation branch has begun a three-year work plan involving various security and privacy initiatives that aim to raise the profile and awareness of privacy in the Ministry and to assist program areas to manage their privacy responsibilities. The branch is also currently working on clarifying its role relative to that of the OCIO and the Ministry's Information Management and Knowledge Services branch.

The recent appointment of a Health Information Privacy Security and Legislation branch employee as the Ministry's Chief Privacy Officer is a major step towards improving governance. Previously the Ministry lacked a high profile champion for privacy inside the Ministry. Without profile-raising for privacy issues, employees may not seek advice on privacy and security when it is needed.

Ministries that hold and process a large volume of sensitive personal information require a dedicated lead or subject matter expert and sufficient resources to be responsible for management and direction of the privacy management program. These include the Ministry of Health, Ministry of Children and Family Development, Ministry of Social Development and Social Innovation, Ministry of Education, Ministry of Advanced Education and the Ministry of Technology, Innovation and Citizens' Services.

There are some functions that require a corporate approach. These include, for example, leading cross-government and legislative initiatives, developing corporate policy, training and operational tools, and providing corporate direction and ensuring consistency in the implementation of legislative requirements. However, there is operational privacy work that requires privacy expertise combined with detailed and specific knowledge about the structure, programs, personnel and information holdings of the Ministry. These operational responsibilities could include:

- establishing and implementing program controls;
- assessing and revising program controls on an ongoing basis;

- creating Ministry and program specific privacy policies and procedures;
- designing and implementing Ministry and program specific employee training and education;
- monitoring and auditing, with documentation, implementation of the privacy management program;
- creating inventories of personal information banks;
- managing privacy breaches;
- writing privacy impact assessments;
- providing privacy advice to Ministry employees;
- representing the public body in the event of an OIPC investigation; and
- demonstrating leadership within the public body in creating and maintaining the desirable culture of privacy.

It is important for each public body to assess the resources necessary to ensure legislative compliance and good privacy practices. This is an issue I intend to pursue in the months to come.

RECOMMENDATION 7:

The roles and responsibilities for privacy belonging to the OCIO and branches throughout the Ministry should be documented and effective overall leadership for the Ministry's privacy management program clarified. There is a particular need to enhance the Ministry's internal privacy resources.

Essential privacy policies

For a public body to implement an effective privacy management program, it needs to develop a suite of key policies and procedures that address its obligations under FIPPA. The OCIO and the Ministry have a large number of policies that promote compliance with FIPPA. These are complemented by the general standards for employees contained in the Oath of Employment, the Standards of Conduct and Information and Communications Technology Policy.

However, there is no Ministry privacy policy that establishes the basic principles of privacy for Ministry employees. Such a policy would be a general statement on the Ministry's approach to privacy; it would provide simplicity and clarity thereby aiding privacy understanding. A Ministry's privacy policy could cross-reference to all these other policies that touch on aspects of privacy.

There is also no Ministry-wide process for ensuring employees are aware of privacy policies and receive annual privacy training. The Health Information Privacy, Security and Legislation branch has recognized this deficiency and has plans to develop a Ministry privacy policy and a policy of confirming, on an annual basis, whether employees have received privacy training.

RECOMMENDATION 8:

The Ministry should develop a Ministry privacy policy that establishes the basic principles of privacy for Ministry employees.

There are several policies on the collection, use and disclosure of personal information that apply generally to ministries, but there is little guidance about the collection, use and disclosure of personal information for research purposes. The July 2012 data access policy of the Information Management and Knowledge Services branch contains some guidance on the general Ministry approach to access to information by Ministry employees, but does not contain specific guidance regarding use or disclosure of information for research. The Ministry should have a clear policy that provides transparency and clarifies expectations for researchers and data stewards about the kind of information that the Ministry can provide and the requisite privacy and security risk management regimes that need to be in place.

RECOMMENDATION 9:

The Ministry should ensure that the Ministry's privacy policy specifically incorporates the collection, use and disclosure of health information for research, including addressing when it may be appropriate to release personal information for health research under s. 35 of FIPPA. It should indicate the kind of information that the Ministry can provide to researchers and the security requirements that need to be met.

Delays in responding to research requests

A Privacy Management Program is about managing risks of unauthorized disclosure of personal information. A particular privacy risk at the Ministry is the difficulty that health researchers have faced in obtaining access to data.

On June 25, 2012, I hosted a roundtable discussion on access to data for health research. The roundtable concluded that while privacy laws posed no barriers to access to personal information for legitimate research purposes, there were issues with the Ministry's handling of data access requests. There was general agreement that the process for approving access was bureaucratic and cumbersome, likely the result of risk-averse data stewards concerned with avoiding privacy breaches at the expense of the public interest in scientific discovery.[18]

Information obtained through this investigation supports that conclusion. Some applications we reviewed had taken more than a year to approve, even though they did not involve any identifiable personal information.

While there is no definitive evidence as to the particular reasons for the disclosures of research data discussed in this report, there is anecdotal evidence that some individuals became frustrated with the delays in processing their data requests and further delays in obtaining access to data that the Ministry had approved for disclosure. The circumstances surrounding the breaches present similarities to a pattern of attempts to work around the lengthy approval process that was apparent in the documentation the investigation reviewed. I note that, if this was the case, it does not excuse anyone for obtaining access to personal health data through unauthorized channels. However, in my view, a more streamlined process for access, combined with clear privacy obligations, would remove any impetus for researchers to seek alternative avenues of access to data outside of the formal approval process.

The Ministry has increased use of the PopData BC Secure Research Environment for information access. As a result of the breach, the application process and form has been further revised. PopData BC now coordinates all information access request applications. This goes some way to addressing the need identified in the Report of the Health Research Roundtable[19] for streamlined and more efficient processes for dealing with information access requests.

[18] This issue was also identified in the Report of the Health Research Roundtable available at: http://www.oipc.bc.ca/special-reports/1483.

[19] http://www.oipc.bc.ca/special-reports/1483.

RECOMMENDATION 10:

The Ministry should continue to streamline its information access request approval and delivery processes to reduce time delays in access to information for health research.

Education and awareness programs

The Core Manual requires new employees to receive privacy and information management training. The OCIO is responsible for the government-wide mandatory training, which the BC Public Service Agency provides through an online course. This training consists of an Information Sharing and Privacy course, launched in September 2010 for all employees, and a specialized course, launched in September 2011, tailored for directors, managers and supervisors.

In addition to the Government mandated training, following the breach the Ministry is delivering its own mandatory privacy and information security education. The Ministry has delivered "Information Management, Privacy and Security – A Management Perspective" to executive directors, directors and managers.

The Health Information Privacy, Security and Legislation Branch also manages a Ministry intranet site with links to the mandatory training sessions and guidance materials on a range of privacy and security issues, though most relate to security. The Ministry's employee orientation handbook also contains references to privacy but does not reflect the current governance responsibilities for privacy in the Ministry.

In late 2012, the Deputy Minister of Health issued a memo reminding all employees of the need to complete the mandatory training.

Completion rates for the government wide mandatory training, as at January 17, 2013 are:

Mandatory Training		
	All Employees	Managers, Directors and Supervisors
All Ministries	67%	70%
Ministry of Health	73%	83%

Source: BC Public Services Agency

Recommendation 11:

The Ministry should ensure that employees with access to databases containing personal health information participate in mandatory privacy training sessions and that their participation is documented.

4.0 Conclusions

This investigation highlights weaknesses in the Ministry's security over personal information.

Ideally, the Ministry should work towards a secure research environment in which all Ministry personal information resides, where access privileges can be tailored to individuals, use can be easily monitored and audited and disclosure monitored and controlled.

Implementing a privacy management program would also assist the Ministry to ensure it meets its obligations under s. 30 of FIPPA. In particular, a privacy management program would help clarify privacy governance responsibilities. An overarching privacy policy and a policy on collection, use and disclosure of personal information for research would set clearer parameters for staff and researchers on the privacy and security requirements when access and use of personal information is permitted.

We will contact the Ministry every three months to confirm the progress of the Ministry in addressing the recommendations in this report.

5.0 Ministry Actions Addressing Privacy Deficiencies

The Ministry has already taken the following actions to address the deficiencies that this investigation has identified.

- The Ministry has completed an inventory of information assets in the Ministry, and all local area network folders used by each Ministry division. A detailed review of that inventory is being conducted to ensure the principles of need to know and least privilege are followed, and that permissions granted to employees match their current job functions.

- The Ministry is increasing the amount of information that resides inside the Health*Ideas* data warehouse, which provides the modern systems architecture enabling privacy and security to be managed and monitored.
- The Ministry has streamlined the data access request approval process for external researchers and pledges to make continuous improvements to it. The Ministry is increasingly utilizing a UBC-operated secure research environment, PopData BC, for information access requests from researchers outside the Ministry.
- Information Management and Knowledge Services branch is required to approve any disclosures of data to contracted service providers before a contract is signed.
- The Ministry has commissioned a private consulting firm to support the Ministry in developing a roadmap to enhance data management practices, specifically with respect to privacy and security.
- The Ministry has implemented a Data Research Policy to guide the Ministry on appropriate access to information for research.
- The Ministry has improved its physical, technical and administrative security controls over CCHS survey information, to comply with security requirements required by Stats Canada.
- The Ministry has appointed a Ministry Chief Privacy Officer.
- The Ministry has expanded the role of the Health Information Privacy Security and Legislation branch to provide a greater profile to privacy and security generally in the Ministry. The branch is also currently working on clarifying its role relative to that of the Office of the Chief Information Office and the Ministry's Information Management and Knowledge Services branch.
- The Deputy Minister of Health issued a memo reminding all employees of the need to complete the mandatory training.
- In addition to the Government mandated training, following the breach the Ministry is delivering its own mandatory privacy and information security education. The Ministry has delivered "Information Management, Privacy and Security – A Management Perspective" to executive directors, directors and managers.

- The Ministry is developing online training modules for information management, privacy and security, privacy impact assessments and security threat risk assessments. Further modules will be developed as required.

- The Health Information Privacy, Security and Legislation branch is developing a Ministry Privacy Policy and a policy of confirming on an annual basis whether employees have received privacy training.

6.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

Summary of Findings

FINDING 1: **I find that, at the time of the unauthorized disclosures, the Ministry did not have reasonable security in place to protect personally identifiable information from unauthorized access or disclosure to the standard that s. 30 of FIPPA requires.**

Finding 2: **I find that the Ministry's immediate response to the unauthorized disclosures was reasonable and met the requirements of s. 30 of FIPPA.**

Summary of Recommendations

RECOMMENDATION 1

The Ministry should develop and implement additions to the BC Government policy on the use of portable storage devices to require the use of other, more secure, forms of information transfer. Portable storage devices should only be used as a last resort and must always be encrypted.

RECOMMENDATION 2

The Ministry should ensure user privileges are granted and managed based on the need to know and least privilege principles, ensuring that employees have access only to the minimum amount of personal information they require to perform their employment duties. Access permissions should be assigned consistently and kept up to date.

RECOMMENDATION 3

The Ministry should implement technical security measures to prevent unauthorized transfer of personal information from databases.

RECOMMENDATION 4

The Ministry executive should implement an effective program for monitoring and auditing compliance by employees with privacy controls, and by contracted researchers and academic researchers with privacy provisions in agreements, to enable proactive detection of unauthorized use and disclosure of Ministry information.

RECOMMENDATION 5

The Ministry should ensure that all contracts with contracted researchers and research agreements with academic researchers involving the disclosure of personal health information provide for an appropriate level of security, including privacy protection schedules. These requirements should include limiting the use and disclosure of personal information to specified contractual purposes; taking reasonable security measures to protect personal information; requiring compliance with privacy policies and controls with respect to storage, retention and secure disposal; and requiring notice to the Ministry in the event of a privacy related contractual breach. The Ministry also should use information sharing agreements wherever the substance of an agreement is about information sharing, rather than the provision of services to the Ministry.

RECOMMENDATION 6

The Ministry should develop a comprehensive inventory of all databases containing personal health information. The inventory should be updated regularly and should set out associated information flows relating to collection and disclosure for research purposes.

RECOMMENDATION 7

The roles and responsibilities for privacy belonging to the OCIO and branches throughout the Ministry should be documented and effective overall leadership for the Ministry's privacy management program clarified. There is a particular need to enhance the Ministry's internal privacy resources.

RECOMMENDATION 8

The Ministry should develop a Ministry privacy policy that establishes the basic principles of privacy for Ministry employees.

RECOMMENDATION 9

The Ministry should ensure that the Ministry privacy policy specifically incorporates the collection, use and disclosure of health information for research, including addressing when it may be appropriate to release personal information for health research under s. 35 of FIPPA. It should indicate the kind of information that the Ministry can provide to researchers and the security requirements that need to be met.

RECOMMENDATION 10

The Ministry should continue to streamline its information access request approval and delivery processes to reduce time delays in access to information for health research.

RECOMMENDATION 11

The Ministry should ensure that employees with access to databases containing personal health information participate in mandatory privacy training sessions and that their participation is documented.

7.0 ACKNOWLEDGEMENTS

The Ministry and OCIO cooperated fully with our investigation.

Hamish Flanagan and Pat Egan conducted this investigation and were the primary authors of this report, assisted by other team members.

June 26, 2013

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia