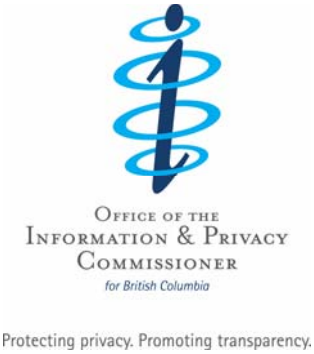

AUDIT & COMPLIANCE REPORT F15-02

EXAMINATION OF BRITISH COLUMBIA HEALTH AUTHORITY PRIVACY BREACH MANAGEMENT

Elizabeth Denham
Information and Privacy Commissioner

September 30, 2015

CanLII Cite: 2015 BCIPC No. 66
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 66

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

One of the most important dealings citizens have with their government is when they entrust their personal information to health care providers. Whether it involves cancer treatment records, records of a person's hospitalization, mental health treatment, or the results of an HIV test, British Columbians share, by necessity, far more sensitive personal information with the health care system than any other sector.

This report addresses one aspect of B.C.'s complex, multi-party health care system – the degree to which health authorities effectively manage privacy breaches when and where they happen.

Strong privacy protection is a cornerstone of quality of care. Patients will only share sensitive information if they trust it will be kept secure; accurate and complete information is essential to proper treatment. If a privacy breach occurs, citizens can very quickly lose trust in the health care system.

Privacy breach management is an essential part of a comprehensive privacy management program, which includes proper records keeping, appropriate and authorized access to records, explicit sharing protocols, and -- should a privacy breach occur -- proper procedures and appropriate notification of affected individuals.

Through this examination we found that health authorities are doing many things that are consistent with good privacy management. However, we also identified significant gaps that must be addressed.

I trust that this report and our examination of government's breach management program, published earlier this year, will raise awareness among senior administrators of the need for a robust and adequately resourced privacy management program for all health authorities.

I would like to acknowledge the hard work of the privacy officers for B.C.'s health authorities, who play a critical role in protecting patient privacy. I also acknowledge the work of my staff in researching and preparing this important report.

I believe that through appropriately designed privacy management programs, British Columbia's health authorities can be leaders in ensuring the protection of the personal health information in their custody. It's a matter of trust.

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

EXECUTIVE SUMMARY

A privacy breach involves the unauthorized access to personal information, or the unauthorized collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" in British Columbia if it occurs in contravention of the *Personal Information Protection Act* ("PIPA") or the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). Privacy breach management is a key component of a public body or organization's overall privacy management program.

This examination of privacy breach management within B.C.'s health authorities is the second project conducted under the Audit and Compliance Program of the Office of the Information and Privacy Commissioner ("OIPC"). The first was an *Examination of BC Government's Privacy Breach Management*[1] (released January 2015). The OIPC chose health authorities for examination because they collect the most sensitive personal information from British Columbians. Therefore, citizens expect that thorough precautions will be taken to safeguard this information from unauthorized access to or collection, use, disclosure or disposal of personal information.

This examination reviewed the extent of compliance with relevant legislation, OIPC guidelines, and health authority policies and procedures with respect to the management and reporting of privacy breaches. It also makes recommendations to strengthen privacy management practices to ensure that health authorities implement the legislation, guidelines, policies and procedures more effectively.

The examination revealed that, in general, privacy officers within each of the health authorities are performing well, given the breadth of their responsibilities. Findings show that most health authorities have privacy policies in place, conduct audits of user access to health records, and appear to be providing necessary breach notifications in a timely fashion to individuals whose personal health information was involved. However, the examination also revealed that there are some fundamental gaps in the foundation of privacy management programs across most of the health authorities.

The recommendations in the report comprise best practices which, if implemented, along with the provisions outlined in the OIPC's *Accountable Privacy Management in BC's Public Sector* will help to ensure health authorities are in compliance with their legislative obligations for protecting personal information. The recommendations, 13 in total, cover the following topics:

- Governance and Resourcing;
- Compliance monitoring
- Notification and Reporting; and
- Training and Confidentiality Agreements.

1.0 INTRODUCTION

The Office of the Information and Privacy Commissioner ("OIPC") established an Audit and Compliance Program to assess the extent to which public bodies and private sector organizations are protecting personal information and complying with access provisions under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA"). The first two projects within this audit and compliance program comprise reviews under s. 42 of FIPPA and s. 36 of PIPA of privacy breach management programs across the broader public sector.

The first audit was *An Examination of BC Government's Privacy Breach Management*[2] (released January 2015). The second project, reported here, is an examination of the effectiveness of privacy breach management within B.C.'s health authorities.

Effective breach management is important to the citizens of British Columbia. As discussed in the January report,

> Public bodies collect sensitive personal information in order to administer many of their programs. Members of the public are concerned about the protection of their privacy and need assurances that they can trust public bodies to appropriately safeguard their personal information and if it is released in an unauthorized fashion, that appropriate follow up steps are taken. An essential part of building and maintaining public confidence is responding appropriately whenever personal information has been compromised, which includes notifications of affected individuals and reporting to the appropriate oversight authority. Such accountability and transparency are key aspects of effective privacy breach management. (OIPC 2015, p. 8).

Over the past 10 years, the OIPC has received 200 reports of breaches from across the health authorities. This may sound like a large number but the OIPC estimates that these reports comprise less than one percent of the suspected breaches that have occurred. Of particular concern is that health authorities, through the plethora of programs, services and facilities, collect what may be considered the most sensitive personal information about members of the public.

Personal information collected in a health setting may include, in addition to personal identifiers such as name; date of birth; and personal health number and financial records:

- The physical, mental and emotional status of individuals over their lifetime;
- Lifestyle and behaviour;
- Health conditions and concerns;

- History of health care procedures and medication use;
- Results of medical tests;
- Related information about family members and other individuals; and
- Genetic information about individuals and their blood relatives.[3]

The OIPC's 2014 special report, *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector* has detailed several privacy issues and concerns relating to the collection of personal information within the healthcare sector. Some of these concerns relate to the patchwork of laws governing collection, use and disclosure; the need for role-based access controls to ensure appropriate access to patient information; complex and multiple purposes for disclosure of health records; appropriate governance and accountability; and the need for robust privacy management programs.

Considering the particularly sensitive nature of health records and the structure of health care systems and services, citizens expect that additional precautions will be taken by health authorities to safeguard this information from unauthorized access to or collection, use, disclosure or disposal of personal information.

Governments have responded to citizens' concerns regarding the security of health records. Virtually all provinces and territories already have or intend to shortly pass personal health information protection legislation. B.C., Quebec and Nunavut have yet to enact legislation specific to the health sector.

In B.C., health sector privacy legislation has been recommended by the OIPC. In its 2014 report, *A Prescription for Legislative Reform*,[4] the OIPC called for government to "enact new comprehensive health information privacy law at the earliest opportunity." The report recommended requirement for breach reporting and notification:

> A legal requirement would help to ensure that this Office is advised of a privacy breach on a consistent basis so that this Office can monitor and provide advice on such issues as the appropriate notice that should be given to individuals. Given the amount and nature of personal health information that could be disclosed in a privacy breach involving EHRs, it should be a requirement in health information privacy law that this Office be notified. The law should also provide for notification of affected individuals and the public, if there is a risk of significant harm (OIPC 2014, p. 47).

The absence of mandatory breach reporting requirements hinders the ability of the OIPC to provide appropriate oversight to ensure that health authorities are meeting their obligations with respect to safeguarding personal information and effectively managing privacy breaches. The reason the OIPC decided to conduct a comprehensive review of breach management practices within health

authorities was due to the sensitivity of personal health information and the lack of an explicit legislative requirement for health authorities to report breaches.

The absence of legislated mandatory breach reporting makes reviewing the health authorities difficult. However, given the importance of ensuring breaches of personal health information are handled appropriately, the OIPC has undertaken this examination because of the importance of ensuring executive attention to this important privacy issue.

1.1 Objectives, Scope and Methodology

The key objectives of this examination were to:

- analyze legislation, guidelines, policies and procedures relating to the management of and response to privacy breaches, including requirements to report breaches within the health authorities, to the OIPC, and to affected individuals;
- review the extent of compliance with the legislation, OIPC guidelines, and health authority policies and procedures;
- identify risk factors and trends involved in managing privacy breaches; and
- recommend improvements to strengthen legislation, guidelines, policies or practices.

The OIPC originally planned this examination in two phases. The first phase was a high level policy and process review of breach management practices within all of the health authorities. The second would have been an in-depth review of breach investigative files from one specific health authority. As a result of the findings from phase one, the OIPC determined there was an urgent need to provide recommendations to the health authorities now to better enable them to meet the safeguarding requirements of s. 30 of FIPPA and s. 34 of PIPA. Consequently, the OIPC decided to postpone phase two.

This review was announced and letters were sent to the heads of the health authorities on April 10, 2015. Data was collected for this evaluation during April through June of 2015 and included a review of background materials relating to the legislative context for breach management within the health sector across Canada; a high-level policy and process review of breach management programs within the health authorities; and on-site interviews with key contacts.

The OIPC examiners designed the interview questions to gain a better understanding of:

- services and facilities that exist within each health authority;

- management and investigation of breaches;
- policies and processes related to breaches;
- numbers and types of breaches that occurred;
- level and types of compliance monitoring that existed;
- details regarding the reporting of breaches to the privacy office within the health authorities, to affected individuals, and to the OIPC;
- breach prevention strategies and privacy safeguards; and
- opportunities to improve privacy breach management.

The OIPC examination team has maintained open communication with the chief executive officers ("CEOs") and privacy officers throughout the review and has provided the health authorities with a copy of the draft report and asked for feedback relating to any errors, omissions or misinterpretations.

2.0 BREACH NOTIFICATION AND REPORTING REQUIREMENTS IN PROVINCIAL AND FEDERAL LEGISLATION

A privacy breach involves the unauthorized access to personal information, or the unauthorized collection, use, disclosure or disposal of personal information.[5] Privacy breaches can be unintentional or deliberate and may range anywhere from mail containing personal information being delivered to the wrong individual, to unauthorized access to databases of personal information by employees, to inappropriate disclosure of personal information of patients or clients.

Managing privacy breaches forms part of the duty to protect personal information.[6] Section 30 of FIPPA and section 34 of PIPA govern the responsibility for privacy breach management and establish a public body or organization's obligation to protect personal information. Both FIPPA and PIPA require that entities protect personal information in their custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

FIPPA also prohibits unauthorized disclosure of personal information and contains a requirement that employees immediately report such disclosures to the head of the public body:

> **Unauthorized disclosure prohibited**
> 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.
>
> **Notification of unauthorized disclosure**
> 30.5 (2) 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.

In addition, as discussed in the *Examination of BC Government's Privacy Breach Management*,[7] OIPC investigation reports and guidance documents highlight a need for appropriate and effective privacy breach management;[8] timely notification of affected individuals;[9] and due consideration for reporting breaches to the OIPC in order for entities to meet their legislative obligations.[10]

B.C.'s FIPPA and PIPA do not currently contain explicit language with respect to reporting breaches to the OIPC or affected individuals. However, the following

OIPC reports contain recommendations regarding mandatory breach reporting requirements in legislation:

- Health Sector: *Prescription for Legislative Reform* (April 2014) called for a new and detailed comprehensive health information privacy law that includes, among other things, mandatory breach notification to affected individuals and the OIPC;[11]
- Private Sector: *Submission to the Special Committee to Review the Personal Information Protection Act* (November 2014) included recommendations for the inclusion of mandatory breach notification provisions that define privacy breaches, the threshold and timing for notifications, power for the Commissioner to order notification to individuals, the form and contents of notifications, duty to document breaches, power for the Commissioner to conduct investigations and audits to attach penalties;[12] and
- Public Sector: The Commissioner, in speaking to the Special Committee to Review FIPPA, noted that it is time for the government of B.C. to consider mandatory breach notification and reporting for the public sector and called for a comprehensive systems-based approach to privacy to be written into law.[13]

In addition, the January 2015 *Examination of BC Government Privacy Breach Management*[14] included recommendations that the B.C. Government:

- Establish an ongoing privacy compliance monitoring function;
- Report to the OIPC breaches that could cause harm to, or involve a large number of, individuals;
- Improve documentation and tracking of privacy breaches;
- Update privacy and breach management policies and training; and
- Provide, and increase participation in, ongoing training and awareness of the importance of protecting personal information and breach management processes.

Several other Canadian jurisdictions have drafted or implemented mandatory privacy breach notification and reporting. When public, private and health sectors are all considered, 11 of the 13 provinces and territories, along with the federal government, have some requirement to notify affected individuals or the privacy commissioner of breaches either in legislation or in amendments that have received Royal Assent. Only three provinces have no mandatory breach reporting requirements: B.C., Saskatchewan[15], and Quebec.

Sections of Bill S-4 relating to mandatory breach reporting, once brought into force, will amend the federal private sector *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). While not directly applicable to B.C.'s

private sector, which is covered by PIPA not PIPEDA, these changes will impact relevant private sector organizations for the majority of central and eastern provinces and each of the three territories. Most of these regions also already have specific health sector legislation in place, or awaiting coming into force, that requires mandatory breach reporting. In addition, Newfoundland and Labrador and Nunavut also have such requirements in public sector privacy legislation, with Newfoundland's legislation being the latest region to adopt mandatory reporting. Alberta has its own private sector reporting requirements and is awaiting the coming into force of such requirements for the health sector.

Thresholds in health legislation for notifying affected individuals of a privacy breach and reporting such breaches to privacy commissioners usually cover any occurrence where personal health information is stolen, lost or accessed by unauthorized persons. Yukon sets the thresholds higher in its pending legislative change, noting that individuals should be informed "when there are reasonable grounds to believe that the individual is at risk of significant harm as a result of the security breach."[16] Most jurisdictions also include a requirement to notify individuals for any breach of their personal information or where it is reasonable to believe that the breach creates a "real risk of significant harm" to the individual.

Regardless of whether the expectation is to notify or report any occurrence of a breach or only when there exists a real risk of significant harm, all enactments require that notifications or reports be made as soon as possible and without unreasonable delay to allow individuals an opportunity to mitigate the risk of harm.

Legislative or regulatory requirements concerning the content of notifications are consistent with OIPC's privacy breach guidance document, *Privacy Breaches: Tools and Resources*. This guideline states that notifications should include the following pieces of information:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- Steps taken to control or reduce the potential for harm;
- Future steps planned to prevent further privacy breaches;
- Steps the individual can take to further mitigate the potential for harm;
- Contact information for a person within the organization;
- Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner; and

- Detail regarding contact with the Privacy Commissioner if the public body or organization has already made contact.[17]

Previous OIPC orders and special reports have interpreted s. 30 of FIPPA or s. 34 of PIPA to include consideration of notifying affected individuals as well as the privacy commissioner in order for a public body or a private sector organization to meet its obligations to safeguard personal information. However, having mandatory breach notification and reporting requirements incorporated within legislation would ensure that all public bodies and organizations have a legal duty and can thus be held accountable for protecting the personal information entrusted to them by patients, clients, employees and the public.

3.0 OVERVIEW OF PRIVACY BREACH MANAGEMENT IN B.C. HEALTH AUTHORITIES

Under the *Canada Health Act*, the federal government provides financial support to the provinces and territories. In turn, the provinces and territories are required to provide reasonable access to medically necessary hospital and doctors' services. Governance for the operation of facilities and programs in British Columbia's health authorities is provided for by the B.C. *Health Authorities Act*, which sets out requirements of regional health boards; and the B.C. *Hospital Act*, which governs hospital care.

The Ministry of Health works together with five regional health authorities and a provincial health authority to provide health services to British Columbians. The Ministry sets province-wide goals, standards and performance agreements for health service delivery by the six health authorities. Additionally, the Province has agreements in place with two private sector organizations: the First Nations Health Authority, which in 2013 assumed the programs, services and responsibilities formerly handled by Health Canada's First Nations Inuit Health Branch for the Pacific Region; and Providence Health Care, which provides services within Catholic hospitals in partnership with two of the health authorities. For simplicity, Providence Health Care is also referred to as one of the health authorities throughout this report.

There are also self-governing First Nations, such as Nisga'a and Tsawwassen, who manage the delivery of healthcare within their communities. These health authorities and services have not been included in this examination.

Together, the health authorities included in this examination are:

- Fraser Health
- Interior Health
- Island Health
- Northern Health
- Vancouver Coastal Health
- Provincial Health Services Authority ("PHSA")
- Providence Health Care
- First Nations Health Authority ("FNHA")

Within each health authority there are a variety of programs providing health services to British Columbians, including, for example: assisted living facilities, clinics, community health centres, hospices, hospitals, residential care, adult day care, seniors centres, mental health and addictions services, home care,

laboratories, cancer agencies, the BC Centre for Disease Control, mobile medical units, urgent care units, and outpatient or ambulatory centres.

The health authorities range in size from roughly 500 (“FNHA”) to nearly 30,000 employees (Interior Health). The five regional health authorities serve populations that range from less than 300,000 spread across a vast rural area (Northern Health) to 1.1 to 1.6 million condensed in a highly urban setting (Vancouver Coastal Health and Fraser Health, respectively). Please see Appendix A for further details on population, density, services and geographical regions for each of the individual health authorities.

The five regional health authorities, along with PHSA and Providence Health Care, each have a dedicated centralized privacy office responsible for receiving, assessing, investigating, and managing privacy incidents reported by the program areas within their regions. The FNHA also has a centralized privacy office that investigates privacy breaches and provides advice and guidance to the First Nations bands who have requested their service; however, their oversight does not extend to the First Nations community level.

Most of these centralized privacy offices also provide education to program and facility staff and create policies on information management, breach reporting, privacy and confidentiality. Some also conduct proactive audits of electronic health records systems (“EHR”) to find instances of unauthorized access to patients’ and employees’ personal information.

4.0 EXAMINATION FINDINGS

This section assesses the extent to which health authorities are complying with relevant sections of FIPPA, PIPA, and OIPC direction (as expressed through guidance documents, reports and orders) relating to privacy management programs in general and, more specifically, breach management policies and practices. It should be noted that OIPC examiners did not inspect policies for completeness or compliance with FIPPA or PIPA.

In addition, staff from the health authorities who participated in the interviews are all referred to below as "privacy officers" when they may actually be officers, advisors, analysts, researchers or investigators within the privacy office. As such, throughout this report, the term privacy officer connotes those who play a role with regard to privacy breach management, regardless of their actual title.

Findings are presented in terms of the process for responding to a breach, including:

- detection of breaches;
- tracking and categorization of breaches
- investigation and management of breaches;
- risk evaluation, notification and reporting;
- prevention strategies; and
- compliance monitoring.

4.1 Detection of Breaches

Do breaches have to be reported within the health authority?

FIPPA requires that privacy breaches be reported to the head of the public body. Section 30.5(2) states:

> 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.

The OIPC considers having privacy policies, including a requirement to report breaches, to be a crucial part of privacy breach management. According to the OIPC's *Accountable Privacy Management in BC's Public Sector:*

> A public body must have in place policies and procedures for protecting personal information. An important function of such policies is to inform

> employees of what is required of them in order to protect personal information.[18]

In order to facilitate staff in meeting this obligation, breach reporting to the head of a health authority should be included in the health authority's privacy policies. Each of the eight health authorities reviewed for this examination have a breach reporting requirement embedded in policy, mandating that staff report any suspected or confirmed breaches to a supervisor, service desk and/or directly to the privacy office.

How are breaches reported within the health authority?

There are a variety of ways for health authority employees to report a breach.

All the health authorities' policies and staff state that, upon discovery of a breach, any employee can phone or email details to their privacy office or can report verbally to a manager/supervisor who will then forward those details to the central privacy office. Contact information for the privacy office was included in only half of the policies.

During interviews some privacy officers stated that the *Patient Safety and Learning System* ("PSLS") – a system designed for capturing details of incidents involving patient safety – is also used for identifying breaches. While the PSLS does not have a separate category for breaches, some of the privacy officers noted that they also review entries for incidents that mention breaches of personal information.

In addition to reporting to the privacy office, four of the health authorities' policies also require that any theft or loss of a portable electronic storage device be reported to IT Services.

Are all breaches reported within the health authority?

When OIPC examiners asked privacy officers whether breach reporting was required, they noted that health authorities expect that <u>all</u> breaches be reported.

However, when asked to estimate the percent of suspected or actual privacy breaches that are reported, privacy officers acknowledged it is difficult to determine whether the policy is followed in practice as there is no meaningful way to estimate the extent of non-reporting. Views ranged from optimism that most or all breaches were being reported to belief that not all breaches were being reported. One privacy officer cited snooping and unauthorized disclosures via social media as areas where compliance with reporting policies was lacking.

Two privacy officers expressed the view that the numbers of actual breaches are decreasing, despite an increase in reports of suspected breaches. They also cited an increase in the number of proactive inquiries from program areas about

privacy protection and breach prevention. They cited these trends as evidence that improved training and awareness was reducing the risk of breaches overall.

Are breaches reported within the health authority in a timely fashion?

Only three of the health authorities had policies that included direction as to when reporting should occur. In two of these instances, the policies stated that potential, suspected, or actual breaches should be reported "immediately" while the third indicated that reporting should be "timely, systematic, and effective".

OIPC examiners did not ask the privacy officers about the timeliness of breach reporting within their health authorities. However, staff from FNHA noted that they are establishing and fine-tuning their breach management procedures to inform all staff who to contact because, at the time of the examination, breach incidents were often being reported to other offices within the health authority. Consequently, it has taken time for the reports to reach the privacy officer tasked with managing breaches.

4.2 Tracking and Categorization of Breaches

How are breaches and breach investigations documented?

Staff from each of the health authorities' centralized privacy offices reported that they electronically log breaches reported to their office, along with the subsequent breach investigations. Systems for tracking breaches and investigations varied from simply filing documents (such as breach reporting forms, email communications, notification letters) on a shared drive, to tracking breaches with a Microsoft Excel sheet, Access database, on a SharePoint site, or IT-helpdesk-type ticketing systems.

There appear to be a number of issues with these tracking systems. Generally, the electronic tracking systems for managing breaches appear to be lacking in terms of their ability to:

- track emails, investigators notes and other records related to breaches and breach investigations;
- capture sufficient details regarding breaches;
- categorize or code breaches;
- prompt investigators to follow up with additional or next steps; and
- proactively analyze patterns or trends.

Most of the privacy officers also identified a challenge in using existing electronic tracking systems for case management. Staff from half of the health authorities

reported that they are actively reviewing database applications with more functionality (such as FileMaker) and preparing business cases to acquire case management software within their offices.

Tracking breaches in an electronic system that allows for categorization of breaches and documentation of breach investigations is the first step in being able to provide an adequate compliance monitoring function. Even if the tracking and documentation takes place in a simple database such as Microsoft Excel, it is imperative that health authorities ensure they have adequate documentation and ability to categorize breaches; document investigative processes; and proactively analyze the causes of and potential solutions for breaches that occur within the health authority.

Are there common categories for types of breaches across the health authorities?

Most of the health authorities were able to provide information relating to the number of reported breaches, whether they were suspected or actual breaches; services or facilities involved; and the category or type of breaches that occurred. Interior Health and Northern Health did not provide information relating to the services or facilities where breaches have occurred but provided all other requested information. All other health authorities provided the requested information.

The OIPC examination team found that each of the health authorities used some sort of categorization or coding based on the type of breach or suspected breach. There appeared to be some recurring categories in the statistics provided but there was no common coding system across the health authorities, so OIPC examiners were unable to make comparisons based on prevalence of types or categories of breaches.

Some of the many types or categories included, for example:

- misdirected communications (mail, email or fax);
- administrative error;
- lost or stolen records;
- lost or stolen devices (encrypted or unencrypted);
- records or devices removed from a vehicle;
- unsecured storage, transportation or transmission of personal information;
- records located in a public place;
- inadequate safeguards;
- access or storage outside of Canada;
- inappropriate access (accidental or deliberate);

- sharing personal information for unauthorized purposes;
- inappropriate disclosure to unauthorized individuals;
- inappropriate disclosure via social media, texting or email;
- inappropriate use of photography or recordings;
- incorrect patient information disclosed;
- inappropriate collection or over-collection of personal information;
- inappropriate disposal of personal information;
- network attacks, hacking, phishing, malware; and
- inappropriate use of resources.

Staff from the health authorities noted that it would be useful to have standardized terminology for coding breaches that may be used across all health authorities in order to facilitate the tracking of breaches and communication across health authorities. OIPC examiners agree that such a coding system would be beneficial for all of the health authorities, and suggest that the privacy officers, perhaps through Health Information Privacy and Security Standing Committee ("HIPSSC"), develop a system that will be of use for each of the health authorities across B.C. In developing this common coding system, the OIPC also suggests that health authorities consider separate classification of:

- legislative default (for example, unauthorized access, collection, use, disclosure, or disposal);
- cause of the breach (such as human error, malicious or otherwise purposeful intent, or inappropriate safeguards);
- the means by which the breach occurred (i.e., fax, email, mail, verbal, social media, hacking, lost, stolen, snooping).

What are the common types of breaches that occur across health authorities?

The OIPC examination team found that there is no meaningful way to compare breach statistics across the health authorities. Some health authorities count every misdirected fax in their overall statistics while others do not. Some health authorities have more advanced training and awareness programs which likely contribute to receiving more reports of suspected breaches. In addition, there may be an overlap of breaches counted by different health authorities, particularly in the lower mainland where a service may be provided by one health authority but the patient or employee are associated with a different health authority. All of these circumstances work to skew any statistical comparison of reported breaches across B.C. health authorities.

Based on statistics provided by the health authorities relating to breach categories, however, the most common categories of breaches across the health authorities appeared to be: misdirected communications; human error; lost records; unsecured storage; and inappropriate access.

Misdirected faxes appeared to be the most common type of breach that occurred across the health authorities from 2012 to 2014. According to privacy officers, administrative errors tend to be at the root of fax breaches, where someone has misdialed the number, or a physician's office has moved and not updated their fax number. While some of the privacy officers reported that they investigate every fax breach, others noted that little or no effort is put into investigating these breaches apart from ensuring containment (i.e., that the faxed materials have been retrieved or deleted).

With regard to lost or stolen records and mobile devices, statistics provided by some of the health authorities indicated that this type of breach occurred more commonly in home health and community care programs. Half of the health authorities noted in interviews that there have been issues over the years with home care workers leaving patient records unsecured in their cars, despite policy requiring locked boxes or stating that there should be no movement of physical records.

Some examples of lost or stolen records received by the OIPC over the last few years include:

- A patient care report fell out of a staff members pocket and was lost;
- Theft of medical student's unencrypted laptop containing information relating to 61 patients;
- 32 patient records stolen from physician's car;
- 66 sensitive patient records were in a vehicle and the vehicle was stolen; and
- A video camera was stolen, containing images of 28 patients.

In addition, most of the health authorities noted during interviews that there are still breaches being reported relating to unencrypted portable devices such as laptops or USBs. This is despite the fact that the health authorities have policies requiring encryption and some of them even provide encrypted devices to mobile workers.

Some of this problem may be explained by noting that most physicians, researchers, and interns are not generally employees of health authorities and, thus, may have their own laptop computers and (unencrypted) USBs instead of organizational devices that are encrypted. Mandatory privacy and security training for all persons with access to personal health information, along with policies requiring the use of encrypted devices, is critical.

Health authorities should ensure that adequate physical and technological resources, such as encrypted USBs for electronic records and trunk lock-boxes for physical records, are in place throughout the health authority for transporting personal information.

Of more serious concern to OIPC examiners is the number of occurrences of inappropriate access to electronic heath records by health authority employees and deliberate disclosures via social media and through personal mobile devices like cellular telephones.

With regard to unauthorized access: the numbers of suspected breaches across the health authorities may be higher for breaches involving unauthorized access due to the existence of audit programs looking specifically for inappropriate access by staff. The OIPC examination team understands that not all inappropriate access breaches involve intentional or malicious snooping (for example, access to an online application allowed the personal information of others to be viewed unintentionally by a staff member). As well, the degree of potential harm that could be caused from intentional snooping differs from examples where a staff member may access their own or their child's records to cases of snooping where staff members access records of VIP or other patients out of curiosity or for a malicious intent.

In addition to snooping, the OIPC has serious concern regarding health authority staff deliberately disclosing the sensitive personal information of patients through their own mobile devices and on social media. These types of breaches can be difficult to discover as privacy offices must rely heavily on reports received from other staff who suspect a breach may have occurred. Examples of such breaches received by the OIPC from the health authorities since 2013 include:

- Four incidents of health authority staff posting photos of patients on Facebook or Instagram;
- Three additional incidents of physicians, nurses or LPNs taking photos of patients on their own mobile devices (one inappropriately shared the photo with a colleague); and
- Another nurse commented on Facebook regarding the personal health information of another individual.

In addition to these examples, challenges around staff use of personal mobile devices and email make it extremely difficult for health authorities to safeguard the information in their care and custody. These circumstances violate patients' expectations of privacy. This is a serious issue because snooping in health records and inappropriately disclosing sensitive personal information of patients undermine public trust in the health care system and seriously impact the quality of service from a patient care perspective.

Issues of deliberate snooping and disclosures need to be addressed by the leadership within health authorities as well as the B.C. government. Other governments across the country, as well as other health authorities, are aware of the seriousness of snooping violations within healthcare records. Employees have been fined through courts; suspended or fired from their positions without pay; charged with criminal code sanctions; or otherwise penalized for intentional breaches of personal information.[19] Class action lawsuits have been raised against health authorities due to the systemic nature of snooping breaches. In addition, governments are adding health record snooping as a specific offence and are increasing fine options within their legislation.[20] Cases of deliberate disclosures have not received the same degree of attention as cases of snooping. However, they also need to be addressed with similar sanctions to control such inappropriate actions.

During interviews, most privacy officers stated belief that their IT program controls are adequate to prevent snooping breaches, when combined with audits and training.

The frequency and impact of these types of breaches highlight the importance of adequate privacy safeguards. These safeguards should include adequate training and awareness programs to aid staff understanding of the importance of safeguarding personal information; adequate audit controls to identify and deter snooping; and sufficient electronic and employee resources to detect and manage breaches. In addition, consequences for intentional violations of personal information need to be included in privacy legislation in B.C.

How many people are affected by health authority breaches?

Regarding the numbers of individuals involved in individual breaches, privacy officers from each of the health authorities estimated that anywhere from 50 percent to 99 percent of all breaches affected only one individual. Similarly, privacy officers reported that privacy breaches that include a large number of individuals occur only once or twice a year. Privacy officers defined large numbers as anywhere from five individuals to 30, 100, 400 or more and noted that it depends on the context of the specific breach.

4.3 Investigation and Management of Breaches

What is the investigative process?

Evidence from policies and interviews indicated that the investigative process for breaches varied between the health authorities, with some adhering to the four steps outlined in the OIPC guidelines[21] and others following their own step-by-step processes. For example, PHSA's breach management policy also outlined responsibilities and accountabilities for the various roles taken in a breach investigation.

These additional responsibilities included:

- confirming data elements that have been breached and ensuring that evidence has been preserved;
- following up with witnesses;
- logging and documenting all information collected during the investigation; and
- liaising with external parties (e.g., OIPC, local police, and other health authorities).

In addition, privacy officers noted that supervisors, managers and the human resources department would be included during investigations of inappropriate access, and that IT departments are included when breaches involve the loss or theft of electronic storage devices.

Who leads the investigation?

In privacy offices with a smaller number of staff, the same privacy officer usually investigates all breaches. Other privacy offices, for example Fraser Health, assign different privacy officers to lead investigations. In PHSA, managers of areas where a breach occurs are responsible for the investigation. PHSA policy notes that privacy officers act as facilitators to advise managers on investigative steps. The PHSA privacy officers added that they provide guidance and support throughout the investigation.

What training is provided to investigators?

From interviews with privacy officers, it appears that most breach investigators have learned on the job. However, privacy officers with Fraser Health and Interior Health reported that they have prior investigative experience either working in law enforcement or by taking investigative courses at the Justice Institute of BC. Three of the privacy officers from across the health authorities also mentioned having participated in International Association of Privacy Professionals (IAPP) programs.

Several of the privacy officer mentioned that the HIPSSC group meets monthly and provides privacy staff at the health authorities with opportunities to share techniques they have used in privacy breach investigations within their own health authorities. Privacy officers reported that this group is very beneficial for sharing information and for offering privacy professionals the opportunity to ask questions and compare investigative materials.

Other learning opportunities mentioned by privacy officers include:

- webinars with discussions on privacy;

- breach management sessions provided by the Office of the Chief Information Officer;
- reports and guidance documents published by the OIPC;
- emerging case law; and
- privacy conferences and seminars.

It is important that health authorities provide adequate investigative training to privacy officers or others who are leading breach investigations in order to ensure objectivity, thoroughness, and consistency in investigations

How many investigators are there within the health authorities?

Within the health authorities, the number of privacy breach investigators ranges from one to five individuals. Resourcing appears to be a limiting factor for Vancouver Coastal Health and Northern Health. These offices are staffed by only one or two individuals and, while they do appear to receive support as necessary from risk management and human resources departments, they are still understaffed compared to other health authorities.

The majority of the health authorities were unable to provide definitive information regarding investigative caseloads due to a failure to effectively track breaches. Island Health estimated that a typical caseload for an investigator would be between 30 to 40 files. The average length of time for investigations differs with each breach depending on the complexity and nature of the circumstance.

Resources available for breach management are further constrained by other privacy-related responsibilities that privacy officers have, including:

- establishing and implementing program controls;
- ongoing assessment and revision of program controls;
- creating privacy policies and procedures;
- designing and implementing employee training and education;
- monitoring and auditing, with documentation, implementation of the privacy management program;
- representing the health authority in the event of an OIPC investigation; and
- demonstrating leadership within the health authority in creating and maintaining the desired culture of privacy.[22]

Interviews with privacy officers and documentation provided by the health authorities confirmed these competing priorities. In addition, during interviews, some of the privacy officers noted that they are also responsible for developing

information sharing agreements and privacy impact assessments as well as various access-related duties, including responding to FOI requests and assessing requests for corrections to personal information.

When comparing the number of privacy officers within a health authority to the population of the region or to the number of other staff within the health authority, Vancouver Coastal Health and Northern Health had consistently lower ratios. Under-resourcing has the potential to seriously impact privacy compliance duties in these health authorities.

In the OIPC's *Prescription for Legislative Reform*, the Commissioner noted that:

> To actively champion a privacy management program, the executive should ensure that all resources necessary to develop, implement, monitor and adapt the program are available to the head. Public bodies face competing demands for public resources, which can be scarce. However, compliance with provincial privacy law is not discretionary; adequate funding and support needs to be devoted to privacy compliance.[23]

Similarly, in the OIPC's guidance on public sector accountability, the adequacy of resources was noted as an important piece to ensuring an effective privacy management program.[24]

4.4 Risk Evaluation, Notification and Reporting

4.4.1 Notification of affected individuals

As noted above, part of a public body's duties under s. 30 of FIPPA include determining whether affected individuals should be notified of a privacy breach. Notification of affected individuals can be an important mitigation strategy. Public confidence in health authorities' collection and use of personal information is strengthened when notifications to affected individuals are provided in appropriate cases.

When should affected individuals be notified?

Policies from six of eight health authorities included criteria to aid in deciding when to notify affected individuals of a breach involving their personal information; however, they did not include a specific threshold that triggers a requirement to notify.

The level of detail for making a decision regarding notification varied considerably in the policies, from simply stating that decisions will be made by the privacy office on a case-by-case basis; to providing a full breach risk assessment evaluation matrix (Fraser Health and Island Health).

As noted in the OIPC's examination of breach management in the B.C. government, decisions around notification are challenging:

> Privacy risk evaluation is a difficult exercise because the unique circumstances and context for any given privacy breach can be so variable. The sensitivity of the information is not the only consideration. It is also important to explore the potential uses for the information and who might have had access to it. OCIO policies (as well as OIPC guidelines) do not provide direction as to how to actually conduct the risk evaluation process. There needs to be explanation of how to draw a connection between the personal information involved and the types of harm the individual could suffer from the breach, the probability or likelihood of that harm occurring, and the severity of harm if it did occur.[25]

When asked during interviews how they make decisions regarding notification of affected individuals, privacy officers noted that they make decisions based on:

- the context and extent of the breach and whether the breach was contained;
- the exposure of particular elements of personal information (the personal health number or birth date, specifically);
- whether the breach was caused by carelessness, curiosity or intentional violation of the rules;
- the likelihood that the personal information breached would result in negative consequences for the affected individuals;
- the number of individuals potentially affected by a breach; and
- the need to balance the potential harm that may result from a breach with the potential harm of notification (particularly with regard to vulnerable persons; for instance, those with certain mental health conditions that may compromise their ability to understand, interpret or respond to such notifications).

These factors, although helpful in making determinations about when to notify individuals, do not provide a standard measure that clearly delineates when such notification should occur, leaving decisions of whether to notify affected individuals subjective.

Health legislation in other Canadian jurisdictions makes it mandatory to notify affected individuals, in most cases, any occasion where personal health information is stolen, lost or accessed by unauthorized persons.

Other types of public and private sector legislation (for example, in Alberta, Nunavut, and the not-yet-in-force changes to the *Personal Information Protection and Electronic Documents Act*, or PIPEDA) refer to a threshold that includes a risk of significant harm. There is no such explicit requirement in B.C.'s FIPPA or

PIPA. One of the benefits of having a threshold in legislation is that it would allow entities to have greater confidence in ensuring that they are meeting their duties under the legislation when making decisions about notifying affected individuals.

In addition, the quality of patient care within specific health authorities, as well as public confidence in health information management in general, would be improved with a structured requirement mandated by specific legislation in the health sector.

Are individuals notified when their personal information has been breached?

Where relevant, OIPC examiners asked the privacy officers to estimate the percentage of breaches that included notification of affected individuals. Privacy officers found it difficult to estimate how often they provided notification, although Fraser Health did indicate that they notify in almost every circumstance.

Privacy officers indicated that they provide notifications verbally (face-to-face, telephone, or video conference), by written letter, or a combination of both verbal and written, depending on the circumstances. Factors they considered included the number of people affected, the sensitivity of the situation (for instance, whether a clinician will be involved in notification to a vulnerable patient), and whether the affected individual requested a letter following a verbal notification. Privacy officers from Fraser Health, Island Health, Northern Health and the PHSA indicated that there is often an initial verbal notification followed-up by a written letter.

In most of the health authorities, privacy officers indicated that the program area responsible for the breach and for the patient provides the initial notification to affected individuals. This is consistent with health authority policies that name the program area as responsible for notification. Privacy officers noted that they provide support to program areas in the form of suggesting wording and other direction regarding notification. In most cases, privacy officers also stated that they routinely retain a copy of the notification within their case file documentation.

Are individuals notified in a timely fashion?

As discussed in the OIPC examination of the B.C. government's breach management program, for notification to be effective and to constitute reasonable security, it must be timely enough to allow those notified to mitigate harm. The OIPC guidelines indicate that notification should occur as soon as possible following a privacy breach and within one week following the discovery of the breach.[26] Investigation Report F08-02 found an inappropriate delay of notification of affected individuals to be a failure by the public body to meet its s. 30 obligations.[27]

Only half of the health authorities had policies that included a requirement for the timing of notification. OIPC examiners found that timelines varied from “as soon as possible” to “within three days of the discovery of the breach” to “within one week”. During interviews, most of the privacy officers noted that they provide notification typically within two-to-three business days of the breach, although two privacy officers acknowledged that sometimes it was not possible to do so.

In contrast, Island Health’s privacy policy requires immediate notification if necessary to mitigate harm. The policy also points to a variety of factors, such as the degree of containment, which may impact the timing and nature of notification. Privacy staff from Island Health also reported that notification occurred once there was sufficient information to do so. They noted that it was not helpful to notify individuals before they had sufficient details, so as not to incite fear, and to allow the health authority to explain the specific actions they were taking to contain the breach and/or prevent further similar occurrences.

4.4.2 Reporting to the OIPC

Both citizens and health authorities benefit from the reporting of breaches to the OIPC at the earliest stages of breach management. The OIPC is well placed to help as it has broad knowledge and expertise from both public and private sector experiences. With this knowledge and expertise, the OIPC provides independent and expert guidance on the management of breaches that is best suited to the needs of those involved.

Reporting breaches to the OIPC is an important consideration for health authorities to manage privacy breaches and meet their duties under s. 30 of FIPPA. Effective oversight by the OIPC increases public trust and confidence that the government is appropriately managing and safeguarding personal information. Open, accountable and transparent communication with the OIPC, particularly with regard to reporting breaches that occur, is important for the oversight function and is in the public interest.

When should breaches be reported to the OIPC?

The OIPC expects that public bodies and private sector organizations, as part of their legislated duty to protect personal information under FIPPA and PIPA, will promptly report relevant privacy breaches to the OIPC. Reporting breaches to the OIPC is important in ensuring that entities have taken steps to reduce the potential harm from a breach; and is essential from a trust and accountability perspective. While the legislation does not include an explicit requirement for health authorities to report breaches to the OIPC, the OIPC’s privacy breach guidelines set out factors to be considered in reporting a breach to this office. [28] These factors, though helpful in balancing considerations about when to report to the OIPC, do not provide a standard measure that clearly delineates when reporting should occur. As such, the decision of whether to report breaches to this office is unavoidably subjective.

The majority of health authorities' policies pointed to considerations of whether to report breaches to the OIPC, though there was no mention of a specific threshold or trigger for mandatory reporting to the OIPC. During interviews, privacy officers noted a variety of factors they consider when deciding to report a breach to the OIPC. Some of these included:

- high risk, serious or severe breaches;
- systemic issues;
- large numbers of affected individuals;
- issues that have garnered media attention; and
- whether affected individuals have been notified.

Every privacy officer noted that they consider the potential for risk of harm to affected individuals as criteria for involving the OIPC. However, there did not appear to be a consistent way for health authorities to measure the level of risk. As noted above, two of the health authorities (Fraser Health and Island Health) have produced matrices to assist in making these determinations. Nevertheless, a more definitive measure for use across the public sector would provide a greater level of certainty. A clear standard could help ensure greater consistency in breach reporting and give health authorities greater confidence that their decisions would comply with s. 30 of FIPPA or s. 34 of PIPA.

As discussed in Section 2 of this report, other Canadian jurisdictions have pending amendments or have already implemented legislative change to include thresholds for mandatory reporting of breaches to privacy commissioners:

- Health Information Acts in New Brunswick, Nova Scotia, Prince Edward Island, Newfoundland and Labrador, Northwest Territories, and Yukon;
- Private sector legislation across Canada (Bill S-4 PIPEDA, which is not yet in force) and in Alberta; and
- Public sector legislation in Newfoundland and Labrador, Nunavut, and for federal public bodies via the Treasury Board of Canada Secretariat Directive on Privacy Practices.

These breach reporting models appear to be relatively similar in terms of the threshold for reporting to the privacy commissioner, with sensitive personal information and a reasonable expectation of injury or harm to affected individuals consistently being the trigger. The examples from other jurisdictions may be useful in forming the basis for a clear reporting threshold for use by the health sector in British Columbia. A clear reporting threshold in British Columbia would provide public bodies and organizations with more specific direction and less subjectivity in determining when to report to the OIPC (and when to notify affected individuals) about breaches. This would, in turn, increase public confidence that personal information is being managed properly.

Are breaches reported to the OIPC?

OIPC examiners asked privacy officers to estimate the percentage of breaches they reported to the OIPC. In some cases, privacy officers noted they could not answer the question and would have to consult their statistics. Among others, answers ranged considerably. One privacy officer estimated that less than one percent of breaches were reported to the OIPC; one indicated that only two breaches had been reported to the OIPC in the last three years; and two estimated that they reported to the OIPC between 4 and 6 times per year.

Statistics on the number of suspected or actual breaches that are documented by a health authority compared to the number of breaches reported to the OIPC show that, in fact, this office receives less than one percent of all suspected privacy breaches identified by the health authorities. Due to the differences in the tracking of privacy breaches within the different health authorities, there is no meaningful way to compare across the health authorities in terms of compliance with guidelines on reporting to the OIPC.

Are breaches reported to the OIPC in a timely fashion?

Data was not collected during this examination to determine the timeliness of reporting to the OIPC. However, it is important to note that the Commissioner expects prompt reporting of privacy breaches to the OIPC in cases where reporting is appropriate.[29] The OIPC privacy breach guidelines state that determination of whether it is appropriate to report the breach to the OIPC should be made "generally within 2 days" of the breach.[30]

4.5 Prevention Strategies

After taking initial steps to contain the breach and mitigate potential harms associated with the breach, including notification and reporting, health authorities should conduct more in-depth analysis with a view to preventing future breaches.

OIPC guidance documents point to a review of policies and procedures, an audit of physical and technical security, training, and an eye toward long term safeguards as ways to minimize the potential for further breaches.[31] Examples of preventative measures may include changes to health authority policies or procedures; improved physical security; enhanced technological security; training for staff or service providers; and changes to supervision and/or contracts with service providers or other contractors.

Are preventative measures being identified and implemented?

Prevention is the final step outlined in the OIPC guideline for responding to privacy breaches and is critical in preventing future breaches.[32] All of the privacy officers indicated that they provide recommendations to the program areas as

part of a breach investigation. Only half of the privacy officers confirmed that they follow up on the recommendations provided in order to determine whether the recommendations have been fully implemented. The remaining privacy officers stated that it is not always practical or possible to follow up after a recommendation has been provided by their office.

For instance, privacy officers from Northern Health, PHSA, FNHA and Providence Health Care noted that they do not always follow up on recommendations. Northern Health and PHSA added that the privacy office does not have authority to require implementation. In addition, FNHA distinguished between the health authority and community organizations for which they provide services, explaining that they have mandated authority to compel action within the health authority. This power, however, does not extend to community or band level. The privacy officer from Providence Health Care noted that, with the recent hiring of a privacy advisor, they intend to follow up on recommendations.

Most of the privacy officers stated that they have the authority to make recommendations during a breach investigation regarding simple preventative measures, such as training. Roughly half of the privacy officers noted that they do not have the authority to require that recommendations be implemented. If a program area ignores or chooses not to implement a recommendation, the issue could be escalated to management for enforcement. However, this escalation may not occur consistently enough to ensure implementation of recommendations provided by the privacy office.

Overall, the majority of privacy officers noted that they do not have an adequate level of authority and/or are not strategically positioned within the entity to be able to effect privacy compliance. If a privacy officer does not have the authority to enforce compliance with its privacy management program, then an entity cannot meet its requirements to appropriately safeguard personal information under FIPPA and PIPA. The first building block is the development of a robust and well-thought-out internal governance structure that prioritizes privacy compliance and fosters a privacy-respectful culture.[33]

Training and confidentiality agreements

The majority of the privacy officers stated that privacy and security training is a mandatory requirement within their health authority. FNHA stated that mandatory training is in process.

Privacy officers also noted that most of the training regarding privacy obligations and breach management for staff and physicians is available online. Fraser Health launched an online training module during the June 2015 Privacy Awareness Week, and privacy officers expressed hope that this training would be made mandatory soon as a supplement to their regular mandatory privacy and security training program.

Despite reports of training being mandatory, the majority of health authorities do not track participation rates in privacy training. For example:

- Privacy officers from PHSA stated that tracking is available but not reliable because it is difficult to pull accurate statistics from their learning hub;
- Providence Health Care reported that employees did not always finish the privacy training and the privacy officer stopped following up;
- Privacy officers from Island Health noted that they were able to track participation when training was done in person but online refresher training has not been tracked because the supporting infrastructure does not exist; and
- In Vancouver Coastal, the privacy officer reported that staff must participate in refresher training every two years and that Human Resources is supposed to track participation (and follow up with managers if not completed) but that tracking is not consistent. As of December 2014, the training completion rate was 57.4%.

Interior Health's privacy officer reported that training completion rates were tracked and that only 10% of the staff had completed the 15-minute online privacy training module. The privacy officer added that, while signing the confidentiality agreement was mandatory, privacy training was not.

The privacy officer from Northern Health reported that they ensure employee participation in privacy training by limiting access to pay stubs and leave allotments until annual refresher training has been completed. Staff may opt to skip the requirement one time and would still be able to access their records; however, if they opt to skip, a notice is sent to the privacy office and follow up is conducted with the employee's manager to ensure that training is completed.

With regard to confidentiality agreements, all health authorities, either via policy or during interviews, confirmed that all employees must sign a confidentiality agreement as a condition of employment. However, in some cases, privacy officers reported that the signed agreement contains an attestation that staff have read the policies or completed the training but that there is no way to verify if they have actually done this.

Physicians, radiologists, researchers, students and any others (who may not be employees of the health authority but have access to personal health information within the care and custody of the health authority) may undergo separate processes with regard to confidentiality attestations or privacy and security training. Privacy officers from the majority of health authorities reported that external users are required to participate in regular privacy training and to sign confidentiality agreements prior to being given access to personal information or in order to maintain privilege to practice within the health authority.

The Commissioner has stated that privacy training should be mandatory for all employees and should be ongoing, regular and sufficiently detailed as to equip employees with the knowledge and awareness necessary to meet privacy obligations.[34] To meet these obligations, every person who has access to personal health information in the custody or control of a health authority should have privacy training and should sign a confidentiality agreement prior to being provided access privileges to such information.

The OIPC examination team found the lack of consistency in the tracking of employee privacy education to be a serious issue. Health authorities must ensure that participation in privacy training and comprehension of the material is documented and must follow up to ensure compliance with training requirements. Having staff who understand their responsibilities regarding the protection of personal information and their role in the event of a privacy breach is imperative to ensuring that personal health information is properly managed.

Management within health authorities must implement safeguards that include effective privacy policies, procedures, and practices. These should also include mandatory comprehensive privacy training and awareness programs and initiatives. Without such, not only is management lacking the foundation to create a culture of privacy within the health authority but there exists a significant gap in the protection of personal health information.

What safeguards are in place?

The health authorities have a number of administrative, physical, and technological program controls that are designed to safeguard personal information, whether in electronic or paper form. The success of these controls can vary depending on the ability to enforce compliance and the level of technological capability within the health authority systems. As well, there are challenges around securing paper files, for example, within a hospital setting where multiple parties need immediate access to patient charts or other personal health information.

Some of the administrative security measures mentioned by the privacy officers included:

- privacy and confidentiality policies;
- privacy and security training;
- research agreements;
- information sharing agreements; and
- security threat risk assessments.

Physical security measures noted by the privacy officers included:

- locking doors and cabinets;

- issuing photo identification;
- having rooms that are only accessible using swipe-cards;
- different levels of physical access for users with more or less privileges;
- closed-circuit television cameras; and
- building lock-down methods and protocols.

Physical security measures can be challenging in a healthcare setting because public access is an essential part of the service. For example, PHSA stated that it is different for every building, noting that the Centre for Disease Control requires visitors to check-in with a security guard who will then issue a pass, whereas some of the Cancer Centres are attached to major hospitals which are fully open to public access after-hours and on weekends. In contrast, Vancouver Coastal pointed out that older buildings, such as Vancouver General Hospital, don't have pass-card security.

Privacy officers stated that some of the technological controls utilized within the health authorities include:

- password protection on computer systems containing personal information;
- authentication and access control protocols;
- system flags to protect confidential information within databases;
- organization-issued smart phones or laptops;
- encryption of mobile devices such as laptops and USB sticks; and
- firewalls and anti-virus software.

Technological controls vary between health authorities. Based on the interviews, it appears that all health authorities are in compliance with role-based access requirement from a policy perspective. However, some of the legacy systems and databases still in use do not have the option of having such security protocols installed. In addition, modern EHR systems may be limited in their ability to allow for role-based access authorizations or health authorities may not be employing this capability.

According to the OIPC, health authorities must implement role-based access as a security control.[35] Role-based access protocols restrict user access based on the least-privilege principle, ensuring that users have the lowest clearance possible that will still allow them to complete their authorized work. One privacy officer noted it is important not to frame this issue as an access control model and instead to consider it an "access optimization model" that focuses on optimizing the sharing of relevant and necessary information to enable efficient and effective quality care, while also protecting privacy interests and rights. In

this way, the health authority seeks to ensure a balance between expectations for safe quality patient care and privacy protection.

The OIPC examination team recognizes the importance of ensuring efficient and effective access to required information, while also recognizing that more can be done across the health authorities to protect the sensitive personal health information of patients and other health centre visitors.

Additional challenges with role based access or access optimization are present with the move toward Lower Mainland Consolidation ("LMC"). Fraser Health, Providence Health Care, PHSA and Vancouver Coastal Health, along with the B.C. Ministry of Health, initiated LMC in August of 2009. Some of the intentions of LMC were to affect standardization, collaboration, integration and cost savings. Through LMC, certain services (for example, medical imaging, health information management, facilities management, and protection services) are led by one of the health authorities, with relevant staff transferred to that lead organization.[36] Privacy officers noted that LMC is guided by a master services agreement with schedules for each of the consolidated services and a general health information sharing agreement. Separate privacy impact assessments, security threat risk assessments, and data sharing agreements are in place for any initiatives that require the sharing of personal health information.

Privacy officers did, however, note that program staff are able to sign into other health authorities' systems, which (while allowing for greater work efficiencies) creates a situation where access controls may not be effective. Privacy officers also stated that LMC highlighted inconsistencies in the treatment and discipline of staff who were caught accessing personal health information without being authorized to do so and requested that guidelines be provided with regard to discipline for staff who are caught snooping. OIPC examiners agree that province-wide guidelines may be of assistance for privacy officers and human resource teams within the health authorities but believe that HIPSSC may be better placed to provide this guidance.

In response to general challenges with implementing role-based access within legacy systems and current patient information systems, the Commissioner has previously called for the B.C. government to enact a new detailed and comprehensive health information privacy law that includes, among other requirements, role-based access models (based on need to know and least privilege privacy principles) with as much granularity as possible and attach penalties for users who violate their conditions of access and that audits should be required.[37]

4.6 Compliance Monitoring

According to the OIPC's guidance document, *Accountable Privacy Management in BC's Public Sector*,

> A privacy management program's controls need to include several types of reporting mechanisms. The goal should be to ensure that the Privacy Officer and executive management are informed, on a regular basis, whether the program is functioning as expected, how and why it is not, and of the proposed fixes (p7).

The OIPC expects that public bodies and organizations will proactively analyze and report the root causes of privacy breaches; explore potential solutions to systemic issues; share this information across the health authority; publicly disclose summaries for openness and accountability purposes; and incorporate findings into training programs and other communications.

Are audits of privacy controls conducted?

The OIPC examination team found that health authorities referred to audits of privacy controls in only half of the policies provided for examination. Policy statements ranged from simply noting that reviews and audits of operational areas are to be conducted to more thorough statements citing specific areas that will be reviewed and the steps for undertaking such activities. Audit policies tended to point more toward audits of appropriate access and client privacy than toward audits of safeguards and compliance with security provisions.

The OIPC's *Accountable Privacy Management in BC's Public Sector* [38] states that internal audits of security safeguards should form a key component in a privacy management program. In addition to internal audits of electronic access to client information, an effective audit program will also enable a health authority to determine whether they are complying with their duties under s. 30 of FIPPA or s. 34 of PIPA to protect personal information by making reasonable security arrangements against unauthorized access or disclosure.

When asked whether or not audits are being conducted within the health authorities, all privacy officers noted that there are regular audits of access to electronic health records. Privacy officers within each of the health authorities reported that they conduct regular audits of IT systems (such as EHR database systems like Cerner and Meditech). Most of the privacy officers mentioned reviewing audit log extracts of access to client records over a period of time. They may send the extracts relating to a number of employees to the relevant managers and request a review of the employees' access to ensure that it was consistent with their job duties and respective patients.

Privacy officers from most health authorities noted that the variety of automatic audit controls are limited in utility and require manual follow up. Some privacy

officers noted that they are not satisfied with the audit capabilities and are looking to upgrade their systems. One privacy officer noted that the existing software was just not designed for auditing purposes and noted that it might be useful for health authorities or the provincial government to look into a province-wide solution that permits auditing multiple systems in a single report.

In addition, not all facilities or staff within the health authorities access patient records through an electronic database. For example, some of the rural facilities within Northern Health may not have broadband or cable connection to the health authority's database and access via satellite technology can be sporadic. Reliance on paper records means that electronic audits, whether reactive or proactive, will not be relevant in these areas.

Only the privacy officers of Interior Health and Island Health confirmed that they do on-site physical inspections as part of a routine audit function. Fraser Health, FNHA and Northern Health noted that they have not conducted physical on-site audits or inspections.[39] Privacy officers from Northern Health noted that the rural northern climate makes it difficult to travel to remote locations for in-person assessments. The remaining privacy officers did not provide comment regarding whether or not they conduct physical audits.

It is critical that public bodies and organizations conduct both physical and electronic audits of compliance with policies and safeguards. The quality of patient care includes the safeguarding and appropriate use of personal health information. Physical and electronic audits to identify potential breaches and other weaknesses in security safeguards should be a regular part of any health authority's risk assessment and risk management processes.

The utility and effectiveness of privacy audits could be enhanced by a functional relationship between internal auditors, risk management units, and the privacy office. The expertise and approach from risk management and internal audit may benefit privacy officers in conducting reviews of privacy issues. In turn, closer connection between the privacy office and risk management and internal audit could raise the profile of privacy within these other processes and allow privacy officers to lend their expertise. In addition, greater exposure of privacy issues across the health authority would be of benefit to risk management and, ultimately, to enhancing the quality of patient care.

What types of analyses and reporting are conducted regarding breaches?

Overall, based on interviews with privacy officers, the majority of the health authorities are not conducting regular systematic analysis or reporting of the breaches occurring within their own regions. Exceptions to this include Island Health, Fraser Health and the PHSA.

Island Health appears to have an extensive program for analyzing patterns or themes in breach reports and extend the research beyond their own jurisdiction to consider trends in breaches reported internationally through regular environmental scan.

Island Health's privacy officers indicated that if they find particular issues through environmental scanning, they raise the topics with information stewards within the health authority as a pre-emptive warning and reports may be sent to the executive with messaging regarding how Island Health is performing in comparison. The environmental scan may provide an idea of leading cases (for example, with regard to snooping breaches), how such breaches have been managed by the entities, the sanctions or remedies that were applied post-breach, and how the issues have been managed within Island Health. They also presented an analysis of snooping breaches at a management forum in order to raise awareness about the issue to boost local accountability.

Privacy officers within Fraser Health reported that they analyse breaches on a monthly basis to determine whether there are systemic issues or particular areas of concern. If an issue or concern is raised through the analysis, a briefing note is drafted for review by the executive member responsible for the particular program area to draw attention to the issue and to implement solutions.

PHSA privacy officers noted that they conduct a monthly review of breach categories and meet with specific agencies to discuss relevant themes for that agency. Results of monthly reviews may also be used for developing targeted education. The privacy officer reported that these analyses are provided to the PHSA executive committee on a regular basis.

Privacy officers from other health authorities noted that they do not conduct proactive analysis or produce such reports on a regular basis but indicated that they are aware of the themes or trends in breaches because, due to the small size of the privacy office, they have reviewed all of the breaches that have been reported.

However, the lack of regular analysis of the numbers and types of breaches, the services or facilities where breaches occur, and the themes or trends taking place constitutes a major gap in the privacy management programs within health authorities. This means that health authorities are missing critical opportunities to address the root causes of privacy breaches within their own jurisdictions; and the chance to develop shared learning with staff across their own entities and across the health care sector.

What information gets reported to the head of the health authority?

As discussed in section 2 of this report, s. 30.5(2) of FIPPA requires that employees immediately report unauthorized disclosures of personal information in the custody or control of the public body to the head of the public body. OIPC

guidance dictates that privacy management programs must clearly define when and how a matter is to be escalated, and to whom.[40]

In most cases, the responsibilities for privacy programs have been delegated to the privacy officer. While six of the eight health authorities examined have policy requiring that staff report suspected breaches to the privacy office, heads of the health authorities (generally the CEO) receive little of this information. When asked about the kinds of information they provide to the CEO regarding breaches, most of the privacy officers mentioned that they only report the significant breaches to the CEO, while Fraser Health stated that the CEO is made aware of each breach incident. Interior Health also noted that they report the number of privacy breaches requiring patient notification on a monthly basis.

There is a gap in providing details related to the numbers and types of breaches received by the health authorities. Without this reporting, the head of the health authority may be unaware of systemic issues or resource needs, including additional training or other resources, that may be required to prevent future breaches from occurring.

Is there public reporting?

Similar to the lack of details regarding the numbers and types of breaches being reported to the CEO, there is also no regular public reporting of information relating to breaches, entities responsible, numbers and types, causes, or preventative measures.

As discussed in the examination of the B.C. government's privacy breach management program, detailed public reporting of privacy breach information would provide increased transparency, accountability, and public confidence in the health sector.

5.0 RECOMMENDATIONS

The following recommendations stem from the findings in this report. They comprise a mixture of best practices that, if implemented, will help to ensure health authorities are in compliance with their legislative obligations for protecting personal information. To assist health authorities with implementation of the recommendations, they have been sorted into the following thematic groupings:

- Governance and Resourcing;
- Compliance Monitoring;
- Notification and Reporting; and
- Training and Confidentiality Agreements.

Recommendations: Governance and Resourcing

Health authorities should ensure adequate governance and resourcing by:

1. Reviewing the organizational position and level of authority of the privacy officer within the entity and ensure adequate placement and authority to facilitate the performance of duties.
2. Ensuring that the privacy officer has adequate resources and staff to fulfill the duties of the role.
3. Ensuring that the privacy office is equipped with software to effectively track the reporting of breaches, the progress of breach investigations, and details relating to each breach; and analyze aggregate results.
4. Ensuring breach investigators, whether within the privacy office or throughout the entity, receive adequate training to effectively fulfill the duties of the role.

Recommendations: Compliance Monitoring

Health authorities should establish an ongoing privacy compliance monitoring function that includes:

5. Ensuring fulsome and accurate documentation of privacy breach incidents and investigations; including but not limited to risk evaluation processes and decisions relating to the notification of affected individuals and the reporting of breaches to the OIPC.
6. Following up with program areas to ensure full implementation of prevention strategies and recommendations provided through breach investigation processes.

7. Conducting and documenting regular region-wide analysis relating to the numbers of breaches, services or facilities responsible, types and causes of breaches, and preventative measures undertaken.
8. Conducting regular audits of privacy and security safeguards including:
    a. Compliance with privacy and security policies;
    b. Physical locations and records, including the transport of records;
    c. IT controls; and
    d. Access provisions.
9. Providing detailed information relating to the numbers of breaches, services or facilities responsible, types and causes of breaches, and preventative measures undertaken to the CEO of the health authority on a regular and timely basis.

Recommendations: Breach Notification and Reporting

Health Authorities should adopt the following interim breach notification and reporting requirements:

10. Promptly and directly notify individuals whose personal information was involved in a suspected breach if the suspected breach could reasonably be expected to cause significant harm to the individual.
11. Promptly report all suspected breaches to the OIPC if the suspected breach:
    a. involves personal information; and
    b. could reasonably be expected to cause harm to the individual and/or involves a large number of individuals.

Recommendations: Training and Confidentiality Agreements

Health authorities should require, provide and track the completion of:

12. Mandatory training and routine refresher training to ensure that all staff understand:
    a. the importance of protecting personal information; and
    b. the breach reporting and management processes.
13. Confidentiality agreements to be signed by everyone with access to personal information in the custody or control of the health authority, or to information systems containing personal information, prior to gaining access.

6.0 CONCLUSION

Effective privacy breach management forms part of the duties of public bodies and organizations to protect personal information as contemplated by s. 30 of FIPPA and s. 34 of PIPA. Health authorities employ a vast array of programs and services at a multitude of locations across each of their respective regions. Each of the health authorities in B.C. has developed a centralized model for the majority of their privacy management programs, in particular, breach investigations processes.

Privacy officers from all health authorities across the province have also established a community of practice that meets regularly to coordinate actions, share information, and strengthen the value of the individual privacy management programs.

However, this examination has revealed that there are some fundamental gaps in the foundation of privacy management programs across the health authorities in BC. Namely, findings from this report pointed to a need in many health authorities for:

- stronger governance and leadership in creating a culture of privacy;
- a review of resources to ensure that privacy officers are equipped with the staff and tools needed to build and maintain adequate privacy management programs;
- greater awareness by all staff across the health authorities, through regular mandatory training, regarding their duties and responsibilities for ensuring privacy and security of personal information; and
- increased compliance monitoring and risk assessment across entities in order to identify gaps in privacy management programs and proactively resolve issues before breaches occur.

Many jurisdictions around the world are implementing explicit accountability requirements into their legislation and policies, including mandatory breach reporting for the public sector. It is time to for all public bodies and private sector organizations in B.C. to move from simply reacting to events like breaches to undertaking a strong proactive role. Health authorities need to implement the accountability measures outlined in this report, along with the provisions contemplated in the OIPC's *Accountable Privacy Management in BC's Public Sector*, in order to meet their legislative obligations.

Health authorities hold some of the most sensitive personal information and, as such, leadership, accountability, compliance monitoring and adequate privacy and security training are necessary to preserve and enhance the privacy rights of the citizens of B.C.

7.0 ACKNOWLEDGEMENTS

The CEOs, privacy officers and other staff from each of the health authorities cooperated fully with my office's investigation.

I would like to thank Tanya Allen, Senior Investigator, and Monique LeBlanc, Investigator, who conducted this examination and contributed to this report.

September 30, 2015

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

APPENDIX A: DESCRIPTION OF B.C.'S HEALTH AUTHORITIES

Fraser Health provides a wide range of integrated health care services to more than 1.6 million people living in communities from Boston Bar in the Fraser Canyon down the Fraser River Valley to Burnaby and Delta. It is the largest health authority by population in B.C. Fraser Health employs 27,293 people in its facilities, which include 12 hospitals, one ambulatory centre, and numerous clinics, community health care centres, residential care and assisted living homes.

Interior Health serves approximately 750,000 B.C. residents within a large geographic area covering almost 215,000 square kilometres. This includes larger cities such as Kelowna, Kamloops, Cranbrook, Penticton and Vernon, as well as a multitude of rural and remote communities. A wide range of health services are provided by more than 21,917 employees at 22 hospitals and dozens of service facilities.

Island Health serves more than 765,000 people on Vancouver Island, the Island in the Salish Sea and Johnstone Strait, and in the mainland communities north of Powell River and south of Rivers Inlet. Island Health employs nearly 18,000 staff at 12 hospitals and more than 100 clinics, health centres and care facilities.

Northern Health covers the largest geographical area of the regional health authorities, providing health services to 300,000 people over an area of 600,000 square kilometers from Quesnel to Fort Nelson and including Haida Gwaii. Northern Health's 7,000 employees staff two dozen hospitals and 14 long term care facilities serving British Columbia's northern cities and a large proportion of rural and remote communities.

Vancouver Coastal Health serves more than one million of B.C.'s residents from Vancouver and Richmond up through the Sunshine Coast as far as Bella Bella and Bella Coola. Vancouver Coastal Health has approximately 14,300 employees, 13 hospitals, and several other services and programs such as community-based residential and home health care, and mental health and addiction services.

Provincial Health Services Authority (PHSA) employs approximately 9,600 staff and operates provincial agencies including BC Children's Hospital, BC Centre for Disease Control, BC Emergency Health Services and the BC Cancer Agency. PHSA is also responsible for specialized health services and programs which are delivered in all regions across the province. It provides advice and guidance but does not have authority over regional health authorities. PHSA is unique in Canada as the only health authority having a province-wide mandate for specialized health services.

Providence Health Care is a faith-based non-profit organization that provides services in partnership with Vancouver Coastal Health and the PHSA. With 6,654 employees, the private sector organization operates under an agreement between the Province of B.C. and the Denominational Health Association to operate and manage 11 Catholic hospitals and health service facilities within the coastal region.

First Nations Health Authority (FNHA) is the first province-wide health authority of its kind in Canada. FNHA plans, designs, manages, and funds the delivery of health programs and services to First Nations populations in both urban and rural communities throughout B.C. These community-based services employ nearly 500 people and are largely focused on health promotion and disease prevention but do not replace the roles or services of the regional and provincial health authorities.

Endnotes

[1] Office of the Information and Privacy Commissioner. 2015. *An Examination of BC Government Privacy Breach Management*. www.oipc.bc.ca/special-reports/1749.
[2] Office of the Information and Privacy Commissioner. 2015. *An Examination of BC Government Privacy Breach Management*. www.oipc.bc.ca/special-reports/1749.
[3] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector.* https://www.oipc.bc.ca/special-reports/1634. *p. 6.*
[4] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector.* P.19. https://www.oipc.bc.ca/special-reports/1634.
[5] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. https://www.oipc.bc.ca/guidance-documents/1428.
[6] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, pp. 14, 15. (https://www.oipc.bc.ca/guidance-documents/1545).
[7] Office of the Information and Privacy Commissioner. 2015. *An Examination of BC Government Privacy Breach Management*. www.oipc.bc.ca/special-reports/1749.
[8] Office of the Information and Privacy Commissioner. Investigation Report F06-02, paragraph 81. (www.oipc.bc.ca/investigation-reports/1233).
Office of the Information and Privacy Commissioner. Investigation Report F13-02, section 2.2, p 20. (https://www.oipc.bc.ca/investigation-reports/1546).
[9] Office of the Information and Privacy Commissioner. Investigation Report F06-02, paragraph 55. (www.oipc.bc.ca/investigation-reports/1233).
Office of the Information and Privacy Commissioner. Investigation Report F08-02; p 12. (https://www.oipc.bc.ca/investigation-reports/1236).
[10] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, pp 14-15. (https://www.oipc.bc.ca/guidance-documents/1545).
Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*, pp. 7-9. (http://www.oipc.bc.ca/guidance-documents/1428).
Office of the Information and Privacy Commissioner. 2013. *Accountable Privacy Management in BC's Public Sector*. https://www.oipc.bc.ca/guidance-documents/1545.
Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioners of Alberta and Office of the Information and Privacy Commissioners of British Columbia. 2012. *Getting Accountability Right with a Privacy Management Program.* https://www.oipc.bc.ca/guidance-documents/1435.
[11] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector.* https://www.oipc.bc.ca/special-reports/1634.
[12] Office of the Information and Privacy Commissioner. 2014. *Submission to the Special Committee to Review the Personal Information Protection Act*. https://www.oipc.bc.ca/special-reports/1717.
[13] Government of British Columbia. 2015. *Report of Proceedings (Hansard Blues). Special Committee to Review the* Freedom of Information and Protection of Privacy Act. Tuesday, July 21. 2015. http://www.leg.bc.ca/cmt/foi/documents-proceedings.asp#.
[14] Office of the Information and Privacy Commissioner. 2015. *An Examination of BC Government Privacy Breach Management*. www.oipc.bc.ca/special-reports/1749.
[15] The language in section 10(1) Saskatchewan's *Health Information Protection Act* refers to trustees being able to inform affected individuals but does not require mandatory notification: "10(1) A trustee must take reasonable steps to ensure that the trustee is able to inform an individual about any disclosures of that individual's personal health information made without the individual's consent…."
[16] Government of Yukon. 2013. *Health Information Privacy and Management Act*. Section 30(1). http://www.canlii.org/en/yk/laws/stat/sy-2013-c-16/latest/sy-2013-c-16.html.

[17] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*, p. 8. (http://www.oipc.bc.ca/guidance-documents/1428).
[18] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p. 11. (https://www.oipc.bc.ca/guidance-documents/1545).
[19] With information received from Island Health on June 19, 2015: *Table Summary of Prominent Canadian EHR Snooping Breaches Reported in the Media from 2012-2015*.
[20] The Government of Ontario has recommended, in Bill 78, the increase of fines from $50,000 to $100,000 for individuals. The Government of Saskatchewan also announced will make health record snooping a specific offence in the *Health Information Protection Act* later this year.
[21] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. http://www.oipc.bc.ca/guidance-documents/1428.
[22] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p. 6. (https://www.oipc.bc.ca/guidance-documents/1545).
[23] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector. p.5.* https://www.oipc.bc.ca/special-reports/1634.
[24] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p. 6. (https://www.oipc.bc.ca/guidance-documents/1545).
[25] Office of the Information and Privacy Commissioner. 2015. *An Examination of BC Government Privacy Breach Management*. www.oipc.bc.ca/special-reports/1749. Pp 26-27.
[26] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. P.18. http://www.oipc.bc.ca/guidance-documents/1428.
[27] Investigation Report F08-02; pp 12 (https://www.oipc.bc.ca/investigation-reports/1236).
[28] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. p.9. http://www.oipc.bc.ca/guidance-documents/1428.
[29] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, Pp. 14, 15 (https://www.oipc.bc.ca/guidance-documents/1545).
and
Investigation Report F08-02; pp 10.
[30] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. P. 18. http://www.oipc.bc.ca/guidance-documents/1428.
[31] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*.
Pp. 10. http://www.oipc.bc.ca/guidance-documents/1428.
[32] Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*. P. 10. http://www.oipc.bc.ca/guidance-documents/1428.
[33] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector.* p. 5. https://www.oipc.bc.ca/special-reports/1634.
[34] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p.13. (https://www.oipc.bc.ca/guidance-documents/1545).
[35] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p 11. (https://www.oipc.bc.ca/guidance-documents/1545).
[36] Provincial Health Services Authority. 2014. Improving efficiency through Lower Mainland Consolidation: An Overview. http://www.phsa.ca/about-site/Documents/LMCOverviewOct2014.pdf.
[37] Office of the Information and Privacy Commissioner. 2014. *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector. Pp.29-30.* https://www.oipc.bc.ca/special-reports/1634.
[38] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p 6. (https://www.oipc.bc.ca/guidance-documents/1545).
[39] FNHA reported that a privacy and security risk assessment is conducted within specific community sites to identify gaps and provide recommendations.

[40] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, p. 7. (https://www.oipc.bc.ca/guidance-documents/1545).