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

INVESTIGATION REPORT F10-02

REVIEW OF THE ELECTRONIC HEALTH INFORMATION SYSTEM AT VANCOUVER COASTAL HEALTH AUTHORITY KNOWN AS THE PRIMARY ACCESS REGIONAL INFORMATION SYSTEM ("PARIS")

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

March 5, 2010

Quicklaw Cite: [2010] B.C.I.P.C.D. No. 13
CanLII Cite: 2010 BCIPC 13
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-02.pdf

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The electronic health record system at Vancouver Coastal Health Authority ("VCH") known as the Primary Access Regional Information System ("PARIS") was introduced in 2001 for its community-based programs. It is accessed by staff and contractors involved in the delivery of a wide range of health services outside of acute care hospitals. These health services include such things as a newborn hotline, home support for seniors, detox services, and communicable disease control. The personal information contained in PARIS is highly sensitive. It includes diagnoses as well as the case notes of physicians, nurses and counsellors about the treatment they provide to their clients.

As a result of our review of the compliance of the system with the standards required by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), we found that the privacy protection of personal information in PARIS is inadequate. Major deficiencies in implementation of the PARIS software from a privacy perspective are the following:

- an access model that is team-based rather than role-based resulting in too many users having access to too much personal information,

- several data flows of personal information outside of the health authority that are not authorized under FIPPA,
- the security protection for the system when we investigated it was not reasonable given the sensitivity of the personal information and did not meet the FIPPA standard[1], and
- records are stored indefinitely – neither archived nor destroyed when they are no longer needed to provide care.

These deficiencies are serious and are a matter of significant concern. It must be noted, however, that these deficiencies are not a result of the software product itself. Rather, they are due to the lack of a proper privacy lens being applied when it was operationalized in community programs at VCH.

VCH has recently put a good privacy management framework in place and is nurturing a corporate culture of privacy. However, this increased capacity and awareness with respect to privacy issues has not yet resulted in an adequate degree of privacy protection for the personal information contained in PARIS. The Information Privacy Office at VCH needs to have greater influence over the system administration of PARIS.

PARIS is a good example of an electronic database that should be designated as a health information bank under the *E-Health (Personal Health Information Access and Protection of Privacy) Act*. Designation would remedy the lack of authority under FIPPA for certain data flows into and out of PARIS. Designation by means of a legal instrument would also inform the public as to how personal information is being collected, used, and disclosed within the health care system, thereby improving transparency and accountability regarding its privacy protection.

Because of the current privacy management framework at VCH, it is anticipated that VCH will be able to respond to our recommendations in a timely fashion. To date, new privacy and security policies have been triggered by this review and role-based access model pilots have been initiated.

We intend to review implementation of all the recommendations contained in this report after one year.

[1] VCH has since made improvements to the security of the PARIS system in response to an audit recently conducted by the Office of the Auditor General.

List of Abbreviations

BCCDC	BC Centre for Communicable Disease Control
CDC	Communicable Disease Control program area of VCH
E-Health Act	*E-Health (Personal Health Information Access and Protection of Privacy) Act*
EIS	Enhanced Information Security Client
FIPPA	*Freedom of Information and Protection of Privacy Act*
IARS	Income Assessment and Rate Setting
IPO	Information Privacy Office at VCH
IT	Information Technology
MCFD	Ministry of Children and Family Development
MoHS	Ministry of Health Services
OIPC	Office of the Information and Privacy Commissioner for British Columbia
PHSA	Provincial Health Services Authority
PIA	privacy impact assessment
VCH	Vancouver Coastal Health Authority
PARIS	Primary Access Regional Information System

Part I - Purpose and Scope of the Investigation

[1] Personal health information has a special status in that it is the most sensitive type of personal information and is collected as part of a unique relationship between health care providers and individuals. In general, personal health information is only disclosed by a patient to a health care provider because the patient requires health care that the patient believes the provider is qualified to deliver. Were it not for this need and the expectation that the provider can assist, the sensitive personal health information would never be disclosed. The only purpose for the disclosure of personal health information by a patient is to seek and obtain health care.

[2] One of the ethical obligations of every health professional is to protect the confidentiality of patient information. The assurance of privacy is essential for patients to be willing to engage in the frank communication with their health care providers that providers rely on to deliver quality care. Patients assume that their personal health information is kept confidential because it is such a well understood hallmark of the provider/patient relationship.

[3] In an era where technology permits health care providers to utilize a common electronic health record, rather than their own separate paper files, it becomes more difficult to assure privacy protection. An electronic health record system is large and complex, more providers and administrative support staff access the system, and more information about more patients is available faster and easier.

[4] We are well aware of the value of electronic health record systems in facilitating the delivery of efficient, timely, and cost-effective health care services. At the same time, however, privacy is a system design imperative—not only to carry forward the ethical obligations of providers but also to comply with legal obligations with constitutional dimensions. The protection of privacy is a fundamental value in modern democracies and is enshrined in ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*.[2]

The Commissioner's Mandate

[5] British Columbia has two main pieces of privacy legislation – FIPPA, which applies to public bodies and the *Personal Information Protection Act* ("PIPA"), which applies to organizations.[3]

---

[2] *Dagg* v. *Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

[3] There are also other pieces of privacy legislation in BC with specific application to certain databases containing personal health information, including the *E-Health (Personal Health Information Access and Protection of Privacy) Act*; *Pharmacy Operations and Drug Scheduling Act* as it applies to PharmaNet; and *Medicare Protection Act* as it applies to Medical Service Plan databases. (See Appendix B.)

[6] VCH is subject to FIPPA because it is a regional health board designated under s. 4(1) of the *Health Authorities Act* and, as such, is within the definition of a health care body in Schedule 1 of FIPPA.

[7] The Information and Privacy Commissioner for British Columbia ("Commissioner") has a statutory mandate to monitor compliance of public bodies with FIPPA to ensure that the purposes of the legislation are achieved [FIPPA, s. 42(1)]. The purposes, as stated in FIPPA, are to make public bodies accountable to the public and to protect personal privacy by, among other things, giving the public a right of access to records and preventing the unauthorized collection, use or disclosure of personal information by public bodies [FIPPA, s. 2(1)].

[8] We have conducted this investigation of the electronic health record system at VCH known as PARIS pursuant to the statutory authority of the Commissioner to conduct investigations and audits to ensure compliance with any provision of FIPPA on his own initiative [s. 42(1)(a)]. The Commissioner also has the authority to examine the implications for privacy and access of automated systems [s. 42(1)(g)].

> **General powers of commissioner**
>
> 42(1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations and audits to ensure compliance with any provision of this Act, …
>
> (g) comment on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information.

[9] FIPPA also authorizes the Commissioner to exercise the power to conduct inquiries, investigations and audits through ordering attendance of persons to answer questions on oath or produce records, among other means of compelling participation [s. 44].

[10] We advised VCH by a letter dated May 25, 2007 that, under s. 42(1)(g) of FIPPA, this Office would review and comment on PARIS's implications for privacy protection. The letter further stated that we would be looking at the collection, use, disclosure and security of personal information in PARIS and that we anticipated producing a public discussion paper or investigation report following the review.

[11] Over the course of the next year, we conducted our investigation through written and verbal communications and a number of face-to-face meetings with VCH staff, on the issue of the PARIS system's compliance with the personal information collection, use and disclosure rules in Part 3 of FIPPA. In letters

dated September 9, 2007 and May 5, 2008, we identified our preliminary areas of concern with PARIS which included authorization for the collection, use and disclosure of information in the PARIS system as well as the security arrangements for PARIS. VCH provided written responses to our preliminary concerns. At our request, in May and June 2007, VCH provided us with a briefing on the security arrangements for PARIS and completed and returned to us a security checklist.

[12] As a result of VCH's responses to our inquiries about the state of the security arrangements for PARIS, we considered that a more detailed review of the security aspects of PARIS was required. It was at this point that we invited the Auditor General to join in our investigation and to produce a joint report in which the Auditor General would report on the technical security aspects of PARIS and our office would report on the compliance of the PARIS system with FIPPA.

[13] In September 2008, VCH was provided with an Audit Summary Memorandum that outlined the process our offices intended to follow. That memorandum indicated that, among other things, the audit would examine role-based access, information disclosures, audit capacity, information security design and internal governance of the PARIS system. It further stated that the audit would be based on the statutory requirements under FIPPA. For the following 10 months staff from both offices conducted the joint audit.

[14] In July 2009 the Auditor General decided to withdraw from the joint audit and a decision was made by both the Auditor General and the Office of the Information and Privacy Commissioner ("OIPC") to publish separate reports on the same matters as originally planned for the joint report. VCH was advised of this change in process both verbally and in writing on July 23, 2009. Following the dissolution of the joint audit process, we proceeded to complete our review of the PARIS system's compliance with the requirements of Part 3 of FIPPA.

[15] The Auditor General provided us with a copy of his office's detailed management report, "Managing Access and Security to the PARIS System for Community Care Services", in early September 2009. We were of the view that it made the most sense for us to review the Auditor General's findings regarding the security arrangements of PARIS to determine if the security arrangements satisfied the statutory standard of s. 30 of FIPPA. We did not want to unnecessarily put VCH through the time and expense of a second security review, and spend our resources on such a review, when the Auditor General's existing work might be sufficient for our purposes.

[16] We reviewed the findings of the Auditor General with the extensive involvement of an OIPC information security expert. Based on this review, we satisfied ourselves that PARIS did not meet the requirements of s. 30 of FIPPA.

[17] We proceeded to complete our examination of the PARIS system's compliance with Part 3 of FIPPA notably with respect to VCH's privacy management framework. Questions on that aspect of our review were provided to VCH in advance of a two-day site visit in September 2009.

[18] With the sole exception of the privacy management framework at VCH (Part III of this report), our findings are based on information that was gathered up to and including June 5, 2009. After that date, changes made by VCH were noted and are reflected in the italicized text that follows the write-up of our findings and recommendations.

[19] The Office of the Auditor General provided a draft public report to VCH on December 8, 2009 with a timeline for VCH to respond before January 29, 2010. We received and reviewed a copy of that draft report in advance of finalizing our public report.

PARIS Operations

[20] The purpose of this investigation is to evaluate VCH's compliance with the requirements of FIPPA in its collection, use and disclosure of personal information in PARIS. Its scope is an investigation and analysis of the privacy framework in place for PARIS, particularly with respect to the following elements:

- Whether the VCH's privacy management framework at VCH is adequate
- Whether there is authority to collect the personal information that is in PARIS
- Whether the personal information in PARIS is the minimum amount that is necessary for the purpose of delivering health care
- Whether personal information in PARIS is used as permitted under FIPPA
- Whether disclosures of personal information from PARIS are permitted under FIPPA
- Whether the security arrangements for PARIS are reasonable
- Whether the retention of records is appropriate
- Whether the storage of records is inside Canada

[21] This report evaluates the above components of the privacy framework of PARIS in terms of the applicable provisions in FIPPA, which set out the legal obligations of public bodies in British Columbia for their collection, use, disclosure, protection, retention, and storage of personal information. These obligations reflect international privacy standards. They are reflected not only in privacy legislation in other provinces in Canada, but also in all liberal democracies around the world.

[22] PARIS has not been designated as a health information bank under the *E-Health (Personal Health Information Access and Protection of Privacy) Act* ("E-Health Act"). That Act is an enabling piece of legislation under which data flows of personal health information through databases of the Ministry of Health Services ("MoHS") and health authorities can be authorized if those databases are designated as "health information banks".

[23] A ministerial order under the E-Health Act could authorize collection (direct and indirect), use and disclosure of personal health information through PARIS for purposes prescribed in the E-Health Act which are related to the delivery of health services. The health-related purposes that would be permitted for the collection, use, and disclosure of personal health information through PARIS are stated in the Act as follows:

> (a) to identify an individual who needs or is receiving health services;
>
> (b) to provide health services to, or facilitate the care of, an individual;
>
> (c) to identify a person who is providing health services;
>
> (d) to prevent or manage chronic conditions, at the individual or population level:
>
> (e) to facilitate health insurance and health service billing, including for the purposes of
>
> i. a payment in respect of health services or prescribed drugs, devices or pharmaceutical services to be made to or by the government of British Columbia or a public body,
> ii. authorizing, administering, processing, verifying or cancelling such a payment,
> iii. resolving an issue regarding such a payment, or
> iv. audits by a federal or Provincial government payment agency that makes reimbursement for the cost of health services or prescribed drugs, devices or pharmaceutical services;
>
> (f) to assess and address public health needs;
>
> (g) to engage in health services planning, maintenance or improvement, including
>
> i. health service development, management, delivery, monitoring and evaluation,
> ii. compiling statistical information, and
> iii. public health surveillance;
>
> (h) to conduct or facilitate research into health issues;
>
> (i) to assess and address threats to public health.[4]

[24] The OIPC has supported the E-Health Act from its inception because of longstanding concerns about the lack of legal authority for the collection, use, and disclosure of personal health information in and through a number of

[4] E-Health Act, ss. 4 and 5.

databases of the MoHS and health authorities.[5] The OIPC is also supportive of the openness and transparency that will be achieved once there is a publicly available legal instrument in place authorizing these electronic data flows of personal health information.

[25] In recent correspondence with the MoHS, the OIPC has advocated that the E-Health Act should be consistently applied to data flows of personal health information through databases of the Ministry of Health Services and health authorities. It is our view that all other piecemeal statutory provisions governing data flows of health information (see Appendix B) should be repealed in favour of ministerial orders under the E-Health Act.

Overview of PARIS

[26] VCH is one of five regional health authorities in BC with a statutory mandate under the *Health Authorities Act* to deliver health care services within a defined region. Health authorities receive global funding from the MoHS. MoHS sets expectations and performance measures for each health authority.

[27] VCH is responsible for delivering health services to Vancouver, Richmond, North and West Vancouver, along the Sea-to-Sky Highway, the Sunshine Coast and Central Coast. VCH has approximately 30,000 employees and is responsible for major urban acute care facilities such as Vancouver General and St Paul's hospitals, as well as community clinics, research centres and residential care facilities.

[28] PARIS is one of eight core electronic information systems at VCH.[6] It is the clinical information system for all community program areas at VCH. There are approximately 4000 users of the system.

The three primary goals of the system are to:

- improve care and service delivery
- establish a sustainable systems infrastructure for clinical documentation
- provide performance measurement

[29] PARIS is a British commercial "off the shelf" product that has been implemented in phases in VCH community programs beginning in 2001. The protection of the personal information that is contained in the system at VCH does not stem from VCH's choice of this particular software. The results of this

[5] The Commissioner issued an authorization under FIPPA for one Ministry database, the Provider Registry, in 2001 with the proviso that the Ministry seek enactment as soon as is practicable of express statutory authority to indirectly collect data for the Provider Registry. The Commissioner's authorization can be found online at http://www.oipc.bc.ca/orders/section42/apr-19-2001.htm.htm.

[6] The others are CareConnect, Excelleris, CareCast, McKesson, SCM, Sunset and webDiagnostic Imaging.

investigation do not in any way reflect any concerns with the PARIS product itself.

[30] VCH implemented PARIS in its community programs. The community programs and the services they provide are the following:[7]

Home and Community Care

[31] Home and community care services are offered to support seniors and adults with significant health problems to live independently in their own homes. Supported housing is available if required. A residential care facility is considered only when other alternatives are unavailable. These services promote self-care in a client's home and prevent unnecessary hospitalization.

Mental Health Services

[32] Specialized mental health care teams provide help for conditions such as schizophrenia, bipolar disorder, depression, behavioural problems and dementia.

[33] Through multidisciplinary care teams and partnerships with external agencies, mental health program teams provide diagnosis, treatment, individual/group therapy, rehabilitation, consultation, emergency and urgent services and residential services.

Addiction Services

[34] Addiction services range from residential treatment centres to outpatient detox services and provide support for individuals with addictions.

Public Health

[35] A program for infants and young children (ages 0 to 5 years) promotes their optimal physical development, communication and cognitive abilities, healthy emotional attachment and positive social development. Services include hospital liaison, postpartum and newborn home visits and support, newborn hotline, breastfeeding clinics, nutrition information and consultation, parent and infant drop in, child health clinics, family and infant follow-up, safe babies program, building blocks program, prenatal outreach services, dental program, audiology mobile outreach and clinic services, community immunization clinics, regional pediatric team, speech/language assessment and treatment, attention deficit hyperactivity disorder program and vision screening.

[36] The child and youth program (ages 5–25 years) supports the health and well-being of Vancouver residents and their families through a range of community primary health care strategies, such as school health liaison and support, child and family follow-up, school health nutrition support, healthy

[7] VCH Community Background v2 – 5 Aug 09.

schools projects and parent education groups. Services include an audiology clinic, education and support groups, assessment, care planning, treatment and intervention, regional pediatric team services, dental program and health attitudes program. Youth clinics provide health services in a youth friendly environment.

Communicable Disease Control

[37] Services include protection, prevention, follow-up and monitoring. The medical health officer responsible for the program reports to the Provincial Health Officer in the Ministry of Healthy Living and Sport.

Personal information in PARIS

[38] PARIS contains the following types of personal information for each client of a community program at VCH[8]:

- demographic information;
- health care services that the client has received;
- diagnosis; and
- case notes of health care providers.

[39] These types of information are stored in modules. The access control model for PARIS is discussed in Part II below.

[40] Several community programs at VCH do not use PARIS because of resource issues. One program records very little personal information in PARIS because of a very high degree of sensitivity about the services being delivered and the potential for stigma.

[8] Interview at VCH, March 13, 2009.

Part II - Compliance with the *Freedom of Information and Protection of Privacy Act*

1. Collection of Personal Information

A. Authority for Collection

[41] A public body subject to FIPPA may only collect personal information if:

(a) the collection of that information is expressly authorized by or under an Act,

(b) that information is collected for the purposes of law enforcement, or

(c) that information relates directly to and is necessary for an operating program or activity of the public body. [FIPPA, s. 26]

[42] We determined what personal information is collected into PARIS by means of interviews with the Information Privacy Office and Information Technology ("IT") office at VCH, specific queries and screen shots of the system. We found that the following types of personal information are collected into PARIS:

- Names of clients,
- Contact information of clients,
- Personal health numbers of clients,
- Allergies of clients,
- Employment,
- Funding or eligibility for funding,
- Education,
- Languages,
- Case notes relating to treatment of clients,
- Names of family members or friends of clients (known as "associated persons" in PARIS),
- Contact information of associated persons,
- Whether the associated person is receiving health care from VCH,
- Financial information and social insurance numbers of clients.

[43] VCH took the position that its collection of all types of personal information was authorized by s. 26(c) of FIPPA, that is, the collection was directly related to and necessary for an operating program or activity of VCH. We agree that, with

respect to collection of personal information into PARIS, only paragraph (c) is applicable.

[44] There are two elements to satisfying s. 26(c) of FIPPA. The collection must be directly related to an operating program or activity of the public body and the collection must be necessary for the operating program or activity. VCH's operating program or activity is the delivery of health care by community program areas.

[45] In assessing whether personal information is necessary, one considers three factors: the sensitivity of the personal information; the particular purpose for the collection; and the amount of personal information collected, assessed in light of the purpose for collection. FIPPA's privacy protection objective is also relevant.[9]

[46] Considering these factors, we found that the following direct collection of personal information of clients is authorized:

- Names,
- Contact information,
- Personal health numbers,
- Allergies,
- Employment,
- Funding or eligibility for funding,
- Education,
- Languages, and
- Case notes relating to treatment.

[47] With respect to the collection of personal information regarding associated persons, VCH advised that it collects names and contact information for the purpose of contacting associated persons in future if necessary for the provision of care to clients. Considering the above factors, collecting non-sensitive identifying information of associated persons is necessary. VCH also links records regarding the treatment associated persons receive at VCH, where the provision of care to one client is considered by VCH to have an impact on the other. This information is highly sensitive and the linking should only be done in very limited circumstances where it is directly related to and clearly necessary for the care of the client. The collection of personal information regarding the health care the associated person is receiving from VCH should be only the minimum amount of personal information that is necessary for the care of the client.

[9] [2007] B.C.I.P.C.D. No. 15, para. 49.

Recommendation 1

VCH should not collect personal information regarding delivery of health care to an associated person unless it is necessary to deliver health care to a client and only the minimum amount of personal information is collected.

[48] With respect to the financial information of clients, including social insurance numbers, VCH explained that this information is collected on behalf of MoHS for the purpose of allowing MoHS to set the annual income assessment rate ("IARS") for community care clients. In order to set the IARS, MoHS requires this information so that it can obtain net income tax information from the Canada Revenue Agency. VCH discloses the financial information including the social insurance number via an extract of PARIS to MoHS. MoHS then further discloses this information to the Canada Revenue Agency in order to obtain net income tax information which then informs the rate setting decision. VCH did not provide evidence that it collected this personal information for its own purposes.

[49] We initially concluded that this collection by VCH is not authorized because it relates to a program of MoHS and not VCH. VCH does not require financial information and social insurance numbers from its community care clients in order to deliver health services to them. However, a legislative amendment was recently passed by government authorizing this specific collection.[10] It is therefore authorized under FIPPA pursuant to s. 26(a) (expressly authorized by or under an Act).[11]

[50] Based on our investigation, we determined that VCH indirectly collects personal information from a database of MoHS known as the Enterprise Master Patient Index for the purpose of identifying clients. This database contains demographic information and personal health numbers of all individuals receiving publicly-funded health care services in BC.

[51] VCH relies on s. 26(c) of FIPPA (necessary for an operating program or activity) as authority for the collection. However, VCH can deliver community health care without collecting or disclosing personal information to MoHS for the purpose of registration confirmation because PARIS has the capability to check registrations to ensure consistency. Moreover, s. 26(c) does not authorize indirect collection by VCH from the Enterprise Master Patient Index.

[52] FIPPA requires a public body to collect personal information directly from the individual the information is about except in specific circumstances, including when the individual has consented to another method of collection or the collection is necessary for the medical treatment of an individual and it is not possible to collect the information directly from the individual [FIPPA, s. 27].

---

[10] *Continuing Care Act*, s. 5 as amended by *Budget Measures Implementation Act (No. 2) 2009*, s. 6.

[11] This amendment is further discussed below at p. 27-28 in connection with disclosure to MoHS.

[53] We found that this indirect collection by VCH from MoHS is unauthorized because it is without consent and the information could be collected directly from the individual.

[54] This indirect collection by VCH could, however, be authorized in a ministerial order designating the Enterprise Master Patient Index as a health information bank under the E-Health Act. The collection from and disclosure to VCH is for a purpose that is permitted pursuant to s. 4(a) of the Act (to identify an individual who needs or is receiving health services). We acknowledge that a province-wide system operated by MoHS in cooperation with health authorities is effective in ensuring that clients are identified accurately.

Recommendation 2

VCH should stop indirectly collecting personal information from the Enterprise Master Patient Index without authority to do so.

B. Notification

[55] When personal information is collected directly from an individual, public bodies must ensure that individuals are told the purposes for collecting their personal information, the legal authority for the collection, and the contact information for the person within the public body who can answer questions regarding the collection [FIPPA, s. 27(2)].

[56] With respect to PARIS, it is preferable that clients of VCH community programs be informed about the collection of their personal information into PARIS and about the operations of PARIS, including to whom their personal information is disclosed.[12]

[57] VCH provides information to clients about its collection of personal information on its website and in notices. We reviewed the website and notices and found that:

- the information on the "Your Information" pages of the VCH website is incomplete (*e.g.* no mention of the PARIS system and it states the records can be accessed only by the client or approved medical staff)
- a notice posted in 2006 in acute care and community sites is limited to collection

[12] This type of notification is required of organizations pursuant to ss. 23(1)(b) and (c) of the *Personal Information Protection Act*. Given that electronic health records may contain personal information from both public and private sources (*e.g.* physician's offices and/or labs) this should be standard for notification.

- a revised version of the notice (dated July 15, 2008) mentions electronic health information systems and disclosures, including that health or other personal information may be shared with MoHS when authorized by FIPPA

[58] In our view, at the time of the investigation the information provided to clients regarding PARIS was not adequate because there was insufficient information about PARIS operations and disclosures from PARIS.

Recommendation 3

VCH should develop more comprehensive web pages and notices for its clients regarding the collection, use and disclosure of personal information through PARIS. At a minimum, they should include a brief explanation of PARIS, the access model within VCH and the disclosures outside VCH.

Recent improvements have been triggered by this review. A new privacy notice, newsletter, and pamphlet for dissemination to clients have recently been developed that provide more information to clients about the collection, use, and disclosure of their personal information by VCH for the purposes of delivering health care.

A new draft version of a notification sign (November 2009) indicates that personal information may be entered into electronic health information systems and specifically mentions PARIS. It also states the purposes for the collection, use and "sharing" of personal information, including as required by the Ministry of Health and with the Canadian Institute for Health Information for statistical analysis and benchmarking.

2. Use of Personal Information

[59] Under FIPPA [s. 32], a public body may use personal information in its custody or control as follows:

a) for the purpose for which that information was obtained or compiled, or for a use consistent with the purpose,

b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

c) for a purpose for which that information may be disclosed to that public body under ss. 33 to 36.

[60] Personal information in PARIS is primarily used for the purpose for which it was obtained or compiled, that is the delivery of health services. In our review

of PARIS, we found that there is also secondary use of PARIS data for the purposes of:

- assessing eligibility for benefits and services,
- arranging payment for services,
- program evaluation,
- teaching and education of VCH staff including medical students, and
- research.

[61] Secondary use of data for research, planning or other purposes is sometimes known as "health system" use. For secondary use to be consistent with the original purpose for collection, the secondary use must have a reasonable and direct connection to the original purpose for collection and must be necessary for performing the statutory duties of the public body or for operating a legally authorized program of the public body [FIPPA, ss. 32 and 34]. For example, personal information collected by a hospital to assist in treatment decisions would be a primary use. The hospital could not use that personal information to identify cancer patients and target them for donations to a cancer clinic. That would be an inappropriate secondary use of the personal information, which could only be undertaken if affected patients consented to that new use.

[62] Personal information collected for the delivery of health services is often de-identified before it is used for research or planning purposes. For the most part, health planners and administrators do not require access to personally identifiable health data and, in principle, only the minimum amount of personal information that is necessary to accomplish the purpose should be disclosed. If there are data linkages, these can be accomplished using unique identifiers on an anonymized basis.

[63] VCH advised us that data disclosed from PARIS for secondary use within VCH is normally de-identified with the exception of personal information used for program evaluation.

[64] We conclude that secondary use of personal information by VCH for the purpose of program evaluation has a reasonable and direct connection to the delivery of health services. Obviously, it is reasonable for any public body to evaluate the programs it is delivering in terms of efficacy and cost-effectiveness, among other things.

3. Disclosure of Personal Information

[65] A public body must ensure that personal information in its custody or under its control is disclosed only as permitted under FIPPA [FIPPA, s. 33]. Unauthorized disclosures are prohibited [FIPPA, s. 30.4].

[66] Authorized disclosures include those for a use that is consistent with the purpose for which the personal information was initially collected [FIPPA, s. 33.2(a)]. A consistent purpose in relation to an electronic health record system would include the delivery of health services to the individual from whom the personal information was collected and for other related purposes, including health insurance and health service billing. It should be noted that the disclosure must be necessary for the duties or programs of the public body that collected the personal information and not for those of other organizations. Only the minimum amount of personal information that is necessary for the duties or programs may be disclosed [FIPPA, s. 34].

[67] Other relevant authority for disclosures include to an officer or employee of the public body if the information is necessary for the performance of the duties of the officer or employee [FIPPA, s. 33.2(c)] and where the information is necessary for the delivery of a common or integrated program or activity [FIPPA, s. 33.2(d)]. The program or activity must be formally established or recorded in documentation and have a structure that demonstrates that there is an integrated program with another public body.

[68] Disclosure is also permitted with the written consent of the individual [FIPPA, s. 33.1(1)(b) and Regulation, s. 6] or where authorized in other legislation [FIPPA, s. 33.1(1)(c)].

A. Access Control Policy

[69] Disclosures of personal information from PARIS to VCH employees for clinical purposes are authorized under FIPPA because they are necessary for the performance of their duties [FIPPA, s. 33.2(c)]. However, only the minimum amount of personal information necessary for the delivery of services may be disclosed.

[70] To ensure that only the minimum amount is being disclosed to users of PARIS, disclosures must be made in accordance with an access control policy that reflects the "need-to-know" and "least privilege" principles. These principles are defined in the Information Management and Information Technology Management section of the Core Policy and Procedures Manual of the BC Government as follows:

> *Need- to-Know*
>
> A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office.
>
> The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain

> records, listing individuals who may access certain records, or installing access controls on all information systems.
>
> The need-to-know principle is especially important in protecting the privacy of individuals as required by the *Freedom of Information and Protection of Privacy Act*.
>
> *Least Privilege*
>
> A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

[71] In accordance with these principles, an access control policy must determine, for each user, the transactions that the user can make and the data fields which the user can access or update – *i.e.* what access privileges a given user can exercise in a given context.

[72] The national and international standard for an access control model for electronic health records systems is role-based access control. The Canadian Organization for the Advancement of Computers in Health ("COACH") has developed standards for how health information should be protected.[13] It identifies the following three types of access control strategies that can help to ensure the confidentiality and integrity of personal health information:

- role-based control, which relies upon the professional credentials and job titles of users established during registration to restrict users to just those access privileges that are required to fulfill one or more well-defined roles
- workgroup based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access
- discretionary or delegated access control, which provides for users of health information systems who have a legitimate relationship to a patient's personal health information (*e.g.* a family physician) to grant access to other users who have no previously established relationship to that patient's personal health information (*e.g.* a specialist).[14]

[73] The Guidelines go on to say that role-based access control is preferred.

> Health information systems containing personal health information should support role-based access control (RBAC) capable of mapping each user to one or more roles, and each role to one or more system functions. This mapping of users to roles greatly facilitates implementation of the need-to-know principle and also greatly reduces mistakes in user

[13] *Coach Guidelines for the Protection of Health Information*, December 15, 2006.
[14] Ibid., p. 105

> administration that will otherwise occur when individual users are each mapped to a customized set of access privileges.[15]

[74] The Privacy and Security Conceptual Architecture developed by Canada Health Infoway for the iEHR identifies role-based access control as a best practice.

> Best practice is to assign access privileges at the most fine-grained level that is practically possible to ensure that access is granted to the minimum PHI [*personal health information*] required for a user to perform a specific job function related to a specific role. Limitations can come by way of limiting access to the system as a whole, limiting access to specific functions, limiting access to data at different levels such as an entire database, specific data subjects or entities, specific data records, specific data fields within records, and specific data operations in the form of read, add, update, etc.[16]

[75] Where there are a large number of users of a system, the administrative burden of determining access privileges on an individual user-by-user basis would be burdensome. It would be inefficient, expensive and ultimately insecure to maintain and monitor that level of complexity in access controls. Instead, by assigning users to roles defined by functions, the access privileges of each user are commensurate with the user's role. Each of the roles in this shorter list cannot, however, be so broad that the need to know and least privilege principles are violated.

[76] The role that is assigned to a user must be based on the tasks and services the user provides. In the case of users that are practising a regulated health profession, those tasks and services must also be within the scope of practice of their profession. It is important to note that the job title or professional designation of a user is not necessarily determinative of their role. The role must reflect the actual health services that the user is delivering, or supporting the delivery of, to clients. Roles must also include information technology ("IT") system administration.

[77] In accordance with the need-to-know principle, access privileges for each role should be limited by what types of information are needed to perform the functions performed by that role (for example, such types of information as demographic, diagnosis, clinical case notes and financial information).

[78] The role must also be defined in terms of the transactions that users in that role need to be able to perform within the system (*e.g.* search by name and/or personal health number, view, update, enter, etc.).

---

[15] Ibid., p. 105.

[16] Canada Health Infoway, Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture, Version 1.1, June 2005.

[79] Applying the least privilege principle, access should be further limited as much as possible so that users are accessing the least amount of that personal information necessary to perform their job functions in their program areas. At a minimum, users should be limited in terms of the types of personal information that they can access. The users' transactions or access privileges must also be restricted to the least privileges that are necessary for their job function.

[80] In our review of the PARIS system, we found that:

- The personal information contained in PARIS is categorized into modules within the system that are accessible to users through four menus.
- These modules include a central index of identifiers, clinical summary, assessments, diagnosis, case notes and care planning.
- All users of PARIS have:
  - universal access to the central index and clinical summary modules, and
  - team-based access to diagnosis and case notes.

[81] Universal access to the central index and clinical summary violates the need-to-know principle because not all roles need access to all the personal information contained in these modules. The central index includes not only demographic information and personal health number, but also allergies, next of kin, employment, equipment, funding/eligibility, languages, reports, school/education. While all roles require basic identifiers, the additional personal information should be reconfigured into different groupings and made available only to those with a need to know.

[82] The clinical summary module includes information regarding diagnosis, hospital care, instructions for health care, financial and legal instructions, palliative registers, surgeries and procedures, tests and diagnosis, vital signs and waitlists. This personal information should be limited to those users who have a need to know this personal information for the purpose of delivering health services to the individual.

[83] We found that the current model of access to other modules, including diagnosis and case notes, is:

- Team-based rather than role-based
- Teams are multi-disciplinary health care teams which may be comprised of physicians, nursing staff, physical therapists, occupational therapists, counsellors and administrative support staff
- Almost all team members have access to the same personal information
- Team directors can authorize access or removal

[84] This team-based or workgroup-based access control permits too many users to have access to too much personal information. It is not sufficiently granular and does not adequately reflect the need-to-know and least privilege principles. Steps should be taken by VCH to move to role-based access control for PARIS whereby access privileges are determined by job functions rather than membership in a workgroup.

Recommendation 4

A new, more granular, role-based access model for PARIS should be developed and implemented.

This model would include a comprehensive roles matrix that maps job functions with the personal information and privileges required to perform those functions. Roles should be defined at the highest level of specificity and granularity as possible, while still taking into account business and clinical workflows within program areas. The amount of personal information within the various modules should also be reviewed so that, in accordance with the least privilege principle, each role only has access to the minimum amount of personal information necessary to perform their functions.

The role-based access matrix must be fully documented and regularly checked and updated by the Information Privacy Office and IT system administration.

[85] Another necessary access restriction is based on clinical relationship—users can only access the records of clients for whom they are delivering services. Access to the records of any given client should be limited to only those users who are providing clinical care, or supporting the clinical care, of that client. This may be accomplished through limiting access to only those users that have a clinical relationship with the client.

[86] It may also be accomplished through an attestation (or confirmation) by the user confirming that every access to a client's record is for the purpose of providing clinical care of that client. Another way would be to restrict access based on location—users working in a particular clinical setting or program area can only access the records of clients who are receiving services in that setting.

[87] Restricting access to a client's personal information to only those users who have a clinical relationship with that client can be implemented in PARIS by operationalizing a functionality that currently exists. PARIS has a functionality called "restricted caseload" that requires clients to be specifically allocated to

a particular user. This functionality has not been fully implemented by VCH. It was new functionality that was unavailable in the initial version of PARIS and requires resources and time to implement. The restricted caseload functionality can be set at the staff, team or department level.[17]

Recommendation 5

Roles should be further limited to client relationship.

The functionality that exists in PARIS for client allocation should be deployed to the maximum extent possible. We were advised that there may be some challenges where there is a shared model of care and services are provided on a 24 hour basis. In that case, consideration may be given to restrictions based on location with an attestation of clinical relationship.

[88] In response to our enquiries regarding the team-based access control, we were advised that team directors can authorize access to PARIS.[18] In a role-based access control model, access privileges should be assigned by a central body that includes both program and privacy expertise.

[89] Decisions of this central body should be made based on recommendations from senior managers who are familiar with the tasks and services provided by each of their staff and the business and clinical workflows of their program areas. To ensure decisions are made and implemented in accordance with privacy obligations, including the need-to-know and least privilege principles, this central body should be comprised of members of senior executive including the Chief Privacy Officer and the Chief Information Officer.

[90] In a centralized decision-making process for the assignment of users to roles there will be an appropriate segregation of duties and division of responsibilities among the approver of what roles are assigned to what users; the nominators of roles for users; IT administrators of the system; and users themselves. It will also help to establish consistency in the access of users across the various clinics and program areas.

Recommendation 6

Users should be assigned to roles by a central body within VCH with privacy expertise so that the need-to-know and least privilege principles are applied consistently.

[17] VCH Community Background v2 – 5 Aug 09.
[18] Interview, March 12, 2009.

[91] When fully implemented, we anticipate that the cumulative result of these three recommendations will be an access control model that meets both the needs of the users, the expectations of the public in terms of privacy protection and satisfies the requirements of ss. 33.2(a) (consistent purpose) and 33.2(c) (necessary for the performance of duties of an employee) of FIPPA.

Steps taken by VCH triggered by this review include a new role-based access control policy issued on June 5, 2009. Its stated purposes include ensuring that users are permitted to access only system information and services as required to perform their professional duties and based on their functional responsibilities. Policy principles include building privacy and security principles of least privilege and need-to-know access into the design of all systems. Controls include segregation of duties, secondary use controls and maintenance of audit logs. Target date for implementing control objectives is June 1, 2010.

VCH has been piloting a new access model for PARIS with a mental health team and an addictions team. In their initial evaluations, team members raised concerns regarding the extra time involved in client allocations and the impact on workflow and team based care. These concerns will need to be resolved prior to full implementation.

B. External Disclosures

[92] Our review of the disclosures of personal information from PARIS to public bodies outside of VCH is limited to consideration of whether there is authority for such disclosures in FIPPA. The issue is not the merits of the data flows—only their legality.

[93] It should be noted that disclosures from PARIS for health-related purposes could be authorized in a designation order approved by the Minister of Health Services under the E-Health Act.

[94] Our findings with respect to external disclosures from PARIS are based on information provided by VCH, including a flow chart and responses to questions raised in correspondence. We also conducted our own research on data collected by MoHS and the Canadian Institute for Health Information.

[95] We found that there are the following external disclosures from PARIS:

i. to MoHS where demographic information is disclosed via an electronic interface with the Enterprise Master Patient Index for the purpose of delivering health services;

ii. to MoHS for the purposes of planning and evaluation (minimum reporting requirements);

iii. to the Ministry of Children and Family Development (“MCFD”) for the purposes of planning and evaluation;

iv. to the Canadian Institute for Health Information (through MoHS) for the purposes of health research and statistical analysis;

v. to health care providers at Providence Health Care;

vi. to PHSA and BC Centre for Disease Control (PHSA / BCCDC), acting on behalf of the Provincial Health Officer of the Ministry of Healthy Living and Sport, for the purposes of monitoring communicable disease and environmental health issues and trends and providing information and analysis on those issues; and

vii. to professional regulatory bodies for the purpose of supervised audits of practitioners and for checking practice standards.

i. Enterprise Master Patient Index

[96] The Enterprise Master Patient Index is a MoHS database that contains demographic information and personal health numbers of all clients of the publicly funded health system in BC. Personal information is disclosed by VCH to MoHS when it updates the demographic data in the Enterprise Master Patient Index with personal information collected directly from individuals. PARIS has an electronic interface with EMPI and new registrations are sent to EMPI, which compares the information against other registrations within other VCH systems and against EMPI. A hard copy report is sent back indicating any matches in these systems. The purpose of the interface is to "correctly identify individuals within the BC health care system so that electronic health information is accurately linked to the correct individuals".[19]

[97] VCH relied on ss. 33.2(a) (consistent purpose) and 33.2(d) (common or integrated program or activity) of FIPPA as authorities for disclosure for the purposes of confirming registration information through the Enterprise Master Patient Index. In our view, the disclosure is not necessary because VCH can deliver community health care without collecting or disclosing personal information to MoHS for the purpose of registration confirmation. Although the Enterprise Master Patient Index is a sophisticated data matching system, VCH advised that PARIS is also capable of checking registrations to ensure consistency. It is thus not authorized under s. 33.2(a) as it does fit within the definition of consistent purpose set out in s. 34 of FIPPA (that it is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body).

[98] In order to satisfy the requirements of s. 33.2(d) of FIPPA there must be evidence of a common or integrated program or activity, including its structure and mandate and documentation establishing it, the membership and budget. We did not see any evidence of a common or integrated program or activity of MoHS and VCH. Collecting similar information for similar purposes does not render those activities "common or integrated".

[19] Response from VCH to July 23, 2007 question list.

[99] We found that this disclosure of personal information from VCH to MoHS through the Enterprise Master Patient Index is not authorized under FIPPA. It would, however, be authorized if the Enterprise Master Patient Index was designated as a health information bank under the E-Health Act.

ii. Minimum reporting requirements to MoHS

[100] MoHS imposes minimum reporting requirements on health authorities for the purpose of health system and program planning, monitoring programs and system performance and reporting on service activities. Among other things, the Ministry collects personal information from health authorities for its continuing care information management system, client patient information system and the mental health client information system. The former is a legacy system that is being discontinued in favour of new home and community care minimum reporting requirements. VCH also sends extracts from PARIS with identifiers of community care clients to MoHS for the purpose of the Income Assessment and Rate Setting process (IARS).

[101] It is our view that there is no authority under FIPPA for VCH to disclose personal information to MoHS for research or planning or IARS. VCH initially relied on ss. 33.1(1)(e) and 33.2(c) (necessary for the performance of duties) and s. 33.2(a) (consistent purpose) which is problematic because it only authorizes disclosure necessary to operate a program of VCH (not the Ministry). Presumably, VCH could conduct its own research and planning and therefore the disclosure is not necessary to operate a program of VCH. Neither is it necessary to deliver a common or integrated program [s. 33.2(d)] because MoHS does not deliver health services to individuals and VCH does not deliver provincial research and planning services. It appears that the disclosures of personal information to MoHS were not re-evaluated either upon regionalization of the health care system or upon the introduction of PARIS. The creation of new separate public bodies (health authorities) that would be responsible for the delivery of health care services should have provoked a reconsideration of the information requirements of MoHS. Disclosures from PARIS to MoHS should also have been reviewed very carefully at the time PARIS was being implemented at VCH.

[102] In response to concerns raised by this Office in correspondence with VCH, VCH pursued this issue with MoHS in October 2007. In the meantime, given the lack of authority for the disclosure, the Board of VCH made a decision to discontinue disclosing personal information regarding continuing care clients to MoHS.

[103] The decision of the Board prompted the Minister of Health Services to issue a ministerial directive effective February 27, 2009, to health authority board chairs that purported to require health authorities to, among other things, submit

plans by December 1, 2009, for full compliance with data reporting as outlined in the minimum reporting requirements specifications. The legal authority for this ministerial directive is unclear.

[104] Subsequently, MoHS proposed an amendment to the *Continuing Care Act* that would authorize collection and disclosure of the minimum reporting requirements for the purposes of the home and community care program area of MoHS.[20] This amendment was passed during the 2009 Fall Session of the Legislature.[21] Disclosure from PARIS would thus now be permitted under FIPPA since it is authorized by an enactment [FIPPA, s. 33.1(c)].

[105] At the time, this Office expressed its opposition to government authorizing the collection of personal information through an overly broad and obscure amendment in this manner. We advocated that the MoHS database containing continuing care information be designated as a health information bank under the E-Health Act.[22] This is in keeping with our longstanding support for the implementation of the E-Health Act in a consistent and comprehensive manner across all MoHS program areas.

iii. MCFD

[106] MCFD is responsible for the delivery of child and youth mental health services in the Province. MCFD has a client services agreement with VCH to deliver child and youth mental health services for MCFD within the health authority. PARIS is used for the collection, use, and disclosure of personal information pertaining to the delivery of MCFD services.

[107] Personal information is provided to MCFD through MoHS because VCH sends one data file to MoHS as part of the minimum reporting requirements containing information about both adult and youth. MoHS passes on a copy of the youth related minimum reporting requirements to MCFD simply as a matter of efficiency since the information sought from VCH by MCFD for the purposes of program evaluation is already provided to MoHS as part of the minimum reporting requirements.

[108] VCH cited s. 33.2(a) of FIPPA (consistent purpose) as the authority for the disclosure to MCFD. VCH could also rely on s. 33.1(1)(e.1) on the basis that VCH is acting as a service provider to MCFD. We agree that the disclosure to MCFD of personal information that is collected by VCH under the client services agreement is authorized. However, we have concerns with respect to two other disclosures of MCFD data. There is no authority for the disclosure of personal information regarding children and youth receiving mental health services to MoHS. This transfer of data through MoHS is merely for reasons of convenience

[20] The *Hospital Insurance Act* has a similar provision with respect to hospital data (s. 7).
[21] Bill 2, *Budget Measures Implementation Act (No.2), 2009*, ss. 6 and 7.
[22] Hansard, 24 September 2009.

and MoHS is not party to the client services agreement. Nor is there authority for the disclosure of MCFD data to all users of PARIS since not all users are acting in the capacity of service provider to MCFD.

iv. Canadian Institute for Health Information

[109] The Canadian Institute for Health Information ("Institute") is a not-for-profit organization headquartered in Ottawa that collects health data from MoHS, and other organizations from across Canada, for the purposes of health research and statistical analysis. The Institute provides information and analyses of health care services, health spending, health human resources, and population health in Canada to governments and other decision-making bodies in the health sector to assess the effectiveness of different parts of the health system and plan for the future. Its data holdings include a continuing care reporting system containing personal information of residents in continuing care facilities, a discharge abstract database containing personal information of hospital patients and a home care reporting system that contains personal information of clients receiving home care in Canada.[23]

[110] VCH relies on ss. 33.2(a) (consistent purpose), 33.1(1)(e) (employee) and 33.2(c) (officer or employee) of FIPPA as authority for disclosure of personal information to the Institute through MoHS. VCH has no direct legal relationship with the Institute but there is an agreement between the Institute and MoHS. Our view is that there is no authority for the disclosure of personal information from VCH to the Institute. The ministerial directive from the Minister of Health Services to health authority board chairs effective February 27, 2009, indicates health authorities are expected to comply with the Institute's home care reporting system and continuing care reporting system standards. The recent amendment to the *Continuing Care Act*, however, authorizes the collection only "for the proper administration of this Act".[24] Further disclosure by MoHS to the Institute for the purposes of health research or statistical analysis is not authorized by the enactment. It could be authorized should PARIS be designated as a health information bank under the E-Health Act.

v. Health care providers at Providence Health Care

[111] Health care providers at Providence Health Care have been given access privileges to PARIS because they also deliver health care services within the health authority. Consideration has also been given to providing access to PHSA employees who are members of an immunization team.

[112] VCH relies on s. 33.2(d) of FIPPA (common or integrated program or activity) to support these disclosures. It also relies on s. 33.1(1)(e.1) (service provider) for the disclosures to Providence Health Care[25]. VCH submits that it

[23] Personal information in the systems includes demographic, administrative and clinical data.
[24] *Continuing Care Act*, s. 5(3)(a)
[25] In a recent decision of the OIPC, it was held that Providence Health Care is not subject to FIPPA. Ref: [2009] B.C.I.P.C.D. No. 36.

has a unique relationship with Providence whereby there is a high degree of integration, coordination, cooperative planning and information sharing between them. The denominational hospitals and residential care facilities operated by Providence are integral to the delivery of health care services in the area. VCH also submits that immunizing youth and children is a common activity between VCH and PHSA.

[113] We did not have sufficient evidence to conclude that Providence Health Care is acting as a service provider to VCH and that there is a common or integrated program or activity in all cases. This means that disclosure to these entities should only occur with the consent of the client and that Providence Health Care should only have access to personal information of their clients on a case by case basis; not to the whole of the PARIS system. If, in fact, this relationship does exist between these two entities, our concerns regarding access would be alleviated by implementation of new role-based access control and client allocation in PARIS.

vi. PHSA / BCCDC

[114] Pursuant to the Health Act Communicable Disease Regulation, communicable diseases must be reported to a medical health officer appointed by the Provincial Health Officer. Medical health officers work within the Communicable Disease Control ("CDC") program area of VCH.

[115] There are three types of disclosure of personal information from PARIS to PHSA / BCCDC.

(a) personal information pertaining to individuals with sexually transmitted diseases and tuberculosis,

(b) regular weekly transfer of CDC data (excluding case notes), and

(c) disclosures in response to ad hoc requests for the purpose of an outbreak investigation.

(a) Personal information pertaining to individuals with sexually transmitted diseases and tuberculosis are reported by CDC to BCCDC and BCCDC is responsible for the public health follow-up. BCCDC then reports back to CDC. BCCDC has a mandate regarding these disease types that existed prior to regionalization of the BC health care system. Recently, CDC has a role in the follow-up for persons with tuberculosis and these are now recorded in PARIS.

It appears that BCCDC is acting as a service provider to VCH in relation to providing public health follow-up care to individuals with sexually transmitted diseases and tuberculosis. Disclosure to a service provider is authorized [FIPPA, s. 33.1(1)(e.1)].

(b) There is a weekly transfer of data from PARIS to BCCDC from CDC for the purposes of aggregate/statistical reporting, surveillance and program evaluation. The data disclosed to PHSA contains personal information, including contact information. BCCDC does not receive case notes.

The regular disclosure of personal information to BCCDC from PARIS is considered to be a report to the Provincial Health Officer. Medical health officers are required to submit reports of positive test results for communicable diseases to the Provincial Health Officer pursuant to s. 2(4) of the Health Act Communicable Disease Regulation. The purpose for the disclosure of names and addresses of infected persons to the Provincial Health Officer is unclear.

A broad Memorandum of Understanding between the Office of the Provincial Health Officer, MoHS, PHSA, and the BCCDC dated June 27, 2007 states that the BCCDC is responsible for ongoing support of the Provincial Health Officer, the Ministry, and health authorities regarding communicable and environmental related diseases and environmental exposures by, among other things, accessing and receiving information and reports about communicable diseases and health threats.

Personal information may be disclosed by a public body in accordance with an enactment that authorizes or requires its disclosure [FIPPA, s. 33.1(1)(c)]. In our view, it is questionable whether the disclosure to the Provincial Health Officer through BCCDC is authorized or required under the *Public Health Act*.

The primary responsibilities of the Provincial Health Officer are set out in s. 66 of the *Public Health Act* as follows:

> 66(1) The provincial health officer must monitor the health of the population of British Columbia and advise, in an independent manner, the minister and public officials
> (a) on public health issues, including health promotion and health protection,
> (b) on the need for legislation, policies and practices respecting those issues, and
> (c) on any matter arising from the exercise of the provincial health officer's powers or performance of his or her duties under this or any other enactment.

Given the mandate of the Provincial Health Officer in relation to monitoring and providing policy advice on population health, the disclosure of personal information of individuals infected with communicable diseases is arguably not necessary. De-identified or aggregate data regarding the incidence of communicable diseases should be sufficient for his purposes.

It is also unclear whether the implied authority of the Provincial Health Officer to collect under s. 2(4) of the Health Act Communicable Disease Regulation can be validly delegated to BCCDC.

(c) Disclosures in response to ad hoc requests for the purpose of an outbreak investigation that is provincial in scale or for the purpose of an enhanced surveillance policy.

Ad hoc disclosures to BCCDC related to an outbreak investigation would be permitted on the basis of compelling circumstances that affect anyone's health or safety [FIPPA, s. 33.1(m)(i)].

[116] A ministerial order designating PARIS as a health information bank under the E-Health Act would authorize the data flow to BCCDC in a clear and transparent manner.

vii. Professional regulatory bodies

[117] Reports and extracts from PARIS are disclosed to professional regulatory bodies, such as the College of Physicians and Surgeons and the College of Registered Nurses, to assist them in monitoring the quality of care delivered at VCH by their registrants. These disclosures are authorized under FIPPA because they are authorized by another enactment, namely the *Health Professions Act* [FIPPA, s. 33.1(1)(c)].

Recommendation 7

VCH should discontinue disclosing personal information from PARIS to MoHS and the Canadian Institute for Health Information unless authorized under FIPPA. Only de-identified information should be disclosed to:

- **MoHS for the purposes of health system and program planning, monitoring program and system performance and reporting on service activities; and**
- **the Canadian Institute for Health Information for the purposes of health research and statistical analysis.**

Personal information should only be disclosed to health care providers at Providence Health Care with consent. [26]

C. Information-Sharing Agreements

[118] To be FIPPA compliant, public bodies must use information-sharing agreements to govern the disclosure of personal information from one entity to

[26] It should be noted that if these disclosures are necessary for any of the purposes set out in s. 4 of the E-Health Act, they could be authorized in a ministerial order designating PARIS as a health information bank under the Act.

another. An information-sharing agreement sets out the terms and conditions for how the personal information will be collected, used, and disclosed by the entity receiving the data. Information-sharing agreements also enhance the transparency and accountability of public bodies with respect to data flows of personal information and how the privacy of individuals is being protected. Government recently recognized their fundamental importance in a statutory requirement for information-sharing agreements with respect to disclosures from health information banks [E-Health Act, s. 19].

[119] We reviewed a number of information-sharing agreements between VCH and other public bodies in terms of their privacy and security requirements. We found that:

- the data access agreement for the disclosures to MoHS through the Continuing Care Information Management system and the Client Patient Information System provides that the data will be collected, retained, used and disclosed in a manner consistent with FIPPA and relevant legislation,
- the current client services agreement between MCFD and VCH states that personal information will only be disclosed in accordance with the agreement and applicable legislation, including FIPPA,
- the Memorandum of Understanding with the PHSA / BCCDC states the parties agree to "facilitate ready access to the full range of health information available to each other with due consideration and commitment to the protection of privacy and compliance with related legislation".

[120] We conclude that there are information-sharing agreements in place for most external disclosures but that they do not always impose specific or detailed standards for the protection of the privacy and security of personal health information. The agreements should not merely reference broad legislative standards, but specifically state the obligations of the recipients of the data to protect it. Given the particular sensitivity of personal health information, all information-sharing agreements should specify high standards for privacy and security, including encryption, secure storage, retention schedules, and requirements for secure disposal of personal information.

Recommendation 8

VCH should ensure that all information-sharing agreements require recipients of personal health information outside VCH to maintain specific reasonable standards of privacy and security protection.

D. Research Purposes

[121] Personal information may be disclosed under FIPPA for research or statistical purposes provided that the following requirements are met:

a) the disclosure must be reasonably necessary to accomplish the research purpose,

b) any record linkage is not harmful to the individuals that information is about and the benefits to be derived from the record linkage are clearly in the public interest,

c) the head of the public body has approved conditions related to security and confidentiality, and

d) the person to whom the information is disclosed has signed a research agreement. [FIPPA, s. 35(1)(a), (b), (c), (d)]

[122] Contact information may be disclosed for the purposes of health research with the approval of the Commissioner [FIPPA, s. 35(2)].

[123] We found that:

- VCH does not have a secondary use policy in place to ensure the conditions for the use of personal information for research are met
- There is a process in place to handle requests for secondary use for research purposes
- The PARIS Steering Committee must approve any request for use of personal information from PARIS before research may proceed
- Research studies must also be approved by the Research Ethics Review Board of the University of British Columbia in accordance with the requirements of the Vancouver Coastal Health Research Institute

[124] There is a lack of documentation on secondary use policy at VCH. That being said, we are satisfied with the processes that are in place, including a requirement of research ethics board approval. We did not see any evidence that disclosures of personal information for research purposes are not meeting the requisite conditions set out in s. 35 of FIPPA.

Recommendation 9

VCH should develop a comprehensive secondary use policy to ensure that the provisions in s. 35 of FIPPA are met. This policy should include requirements for security and confidentiality and a template for research agreements.

E. Enhanced Information Security Client

[125] An important privacy principle is that individuals should have control over their own personal information to the maximum extent possible. One mechanism that provides an individual with the ability to control their personal information in an electronic system is a "masking" feature. This allows an individual to restrict access to personal information that is collected by the public body. In order for this option to be meaningful, the public body must inform individuals that the option is available; there should not be any barriers for the individual to exercise it; and the individual must be advised of the implications and have access to clinical advice. The ability of a client to mask their personal information is particularly important when its collection is mandatory.

[126] In PARIS, there is an Enhanced Information Security Client ("EIS") flag feature in the system that enhances the ability of clients to control their own personal information in PARIS.

[127] We found that:

- At the time of our investigation, guidelines for EIS (effective July 2008) set out the following criteria for those who could access the EIS:
  - Staff or family member of a staff person
  - Notable person
  - Clients who can demonstrate that the PARIS security model does not provide sufficient security
- Clients were evaluated individually before locking down records.
- Clients were not routinely informed of the option to be considered as EIS (there was no mention of it on the "Your Information" pages on the website of VCH).

Recommendation 10

All individuals should be advised of and have the option to be considered as EIS without having to justify their choice. Individuals should be consistently informed of the option to be flagged as EIS, its implications and how this option is exercised.

Recommendation 11

There should be a clear and more expansive notice to clients on the VCH website and elsewhere about the EIS option. This notice should describe the access model in PARIS and indicate the availability of the EIS option, the process for clients seeking to be flagged as EIS and the implications of being flagged. Clients should also be informed that clinical advice is available if they are considering this option.

We were advised that an EIS sub-group of VCH's Privacy, Security and Confidentiality Working Group is in the process of developing a general policy for EIS that will apply to both acute and community care.

We were provided with a draft document entitled "EIS Requirements and Specifications" dated March 30, 2009. Key principles include:

- *Clients should have some degree of control over access to their personal information*

- *Clients should be informed of the impact and/or consequences of their record not being available to care providers currently and in the future.*

- *The decision to request EIS is personal and confidentiality of the request must be maintained.*

The draft document states that clients will be able to initiate requests at numerous points of contact and at any time. Registration Services will require clients to complete an EIS form but clients will not have to justify their request. Phase 1 deliverables include documenting health service providers with whom clients can consult regarding an EIS request and EIS Education and Awareness communication.

The EIS guidelines were revised in May 2009 to reflect a new policy that is being piloted at VCH. Clients must be informed in writing of the EIS option and not be asked to justify their request or concerns. The client must be aware of how the option limits access to their record and where appropriate the client's physician should be consulted. The preferred process is for the request to be made to the clinician. The client must complete a request form and the request must be approved by the team manager.

A new information sheet indicates that the EIS option is "for clients who have particular concerns about the security of their electronic record, for example, staff receiving services from sensitive programs or public figures".

4. Protection of Personal Information

[128] Section 30 of FIPPA is a statutory obligation imposed on public bodies to protect the personal information in its custody or control. It applies to VCH and the security framework for PARIS.

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

[129] The Commissioner has interpreted the standard of reasonableness in previous investigation reports. In a 2006 report[27], the Commissioner stated:

> [49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
>
> [50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

[130] The nature and level of security will depend on the sensitivity of the information. As was also noted in Investigation Report F06-01:

> [52] The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.
>
> [53] Sensitivity is a function of the nature of the information, but other factors will also affect sensitivity. For example, the sensitivity of medical treatment information for someone who died 70 years ago is less than for someone who died more recently or is living.

[131] We interviewed staff responsible for IT system administration for PARIS, reviewed responses to our security checklist and participated in the analysis conducted by the Office of the Auditor General. We engaged a security expert to assist in our review of the findings and recommendations of the security audit conducted by the Office of the Auditor General.

[132] In our view, security arrangements for PARIS during the period of our investigation did not meet the standard of reasonableness that is required and therefore were not in compliance with FIPPA. Because of the large number, and serious nature, of the deficiencies in security, we have chosen not to elaborate on them in this report.

---

[27] Investigation Report F06-01, [2006] B.C.I.P.C.D. No. 7.

[133] We do, however, wish to highlight certain core security standards for an electronic health information system of this nature. Given the sensitivity and amount of personal health information contained in the system we are of the view that a very high standard of security is reasonable in the circumstances.

[134] The following core security standards were not met:

1. Documented change control procedures approved by management (ISO standard).

   There must be a written record of the procedures and controls that are in place to protect the security of the system. This will allow an assessment to be made as to whether the procedures are being properly executed.

2. Controls to detect, prevent and log unauthorized data exchanges must be in place.

   Activity on the servers must be tracked, logged and reviewed in order for system administrators to monitor the security of the system on an ongoing basis and investigate security and performance issues.

3. Production data must not be used in a development or testing environment.

   Real data containing personal information of identifiable individuals must never be used outside of a fully secured production system. During the development or testing phase of a new system, only fictitious or anonymized data should be used.

4. There must be an entrance and exit strategy for staff, contractors, and third parties.

   As previously discussed in this report, when employees or contractors start working at VCH, they should be assigned roles by a central body within VCH that permits them to access only that personal information they require to perform their job functions in accordance with the need-to-know and least privilege principles. Should an employee or contractor leave their position or discontinue providing services to VCH, their termination and its effective date should be immediately communicated to the system administrator. The system administrator should ensure that access by former VCH employees and contractors to PARIS is disabled as soon as it is no longer required.

[135] Moreover, in addition to the above industry standards applied by the Office of the Auditor General, we are of the view that the following standards are reasonable in an eHealth system:

5. Firewalls should exist along the perimeter as well as being host based. The inbound and outbound rules for all firewalls should be business required and approved by management.

There should be a defense in depth security strategy whereby multiple layers of defense are placed throughout the system to address security vulnerabilities. Defense in depth measures prevent security breaches. They also give an organization time to detect and respond to an attack so that the consequences of a breach can be reduced and mitigated. Firewalls should exist with a default deny policy wherever possible at all layers of the system and not just the perimeter. This would include internal firewalls at the layers of networks and hosts. The rules should be approved by management, and inappropriate access attempts should be detected and monitored.

6. Data should be encrypted both during transmission and storage.

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those given a key to decipher it. In our view, sensitive personal health information contained in an electronic health record system should always be encrypted to reduce the risk of exposure. Encryption should be required both for transport and storage of data.

7. Only approved network services are permitted on all systems and patched to the latest version.

Any network services, including websites or email servers, must be approved by management. Those network services that are run by default by operating systems would have to be turned off unless they are approved.

When a means of attacking the version being used is developed by a hacker (*i.e.* an exploit) and becomes known, that version is fixed through a patch. The exploit then becomes obsolete for newer versions of the software. The system should be upgraded or patched to the latest version that cannot be exploited.

[136] VCH has remedied serious deficiencies in response to the audit conducted by the Auditor General. We intend to monitor and assess efforts made by VCH to continue to implement recommendations from the Office of the Auditor General and meet the core eHealth security standards set by this Office.

The following security policies were issued by the Chief Financial Officer and Vice-President, Systems Development and Performance at VCH on June 5, 2009:

Information security

- *purpose is to ensure that VCH maintains the confidentiality, integrity and availability of information stored or shared on VCH systems*

- *policy is outcome-based and does not set detailed standards*
- *states security requirements must be specified at the design phase of a system on the basis of a risk assessment*
- *control requirements include:*
  - *data must be classified,*
  - *access rights of staff removed upon termination of employment, and*
  - *access control rules must be based on need-to-know and least privilege.*

User identification and passwords

- *sets out requirements to uniquely identify users for the purposes of managing access, including to assign access privileges and audit user activity*
- *the requirements are determined jointly by the Information Privacy Office and Information Management Information Security Services.*

Remote access

- *sets conditions for users requiring remote access to systems and information stored on systems*
- *requirements include two-factor authentication and encryption*

Other policies approved on June 5, 2009 include internet access and acceptable use of information technology. A policy on electronic mail (e-mail) usage policy has been in place since 2004.

5. Storage and Retention of Personal Information

A. Stored in Canada

[137] Subject to specific exceptions, a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada [FIPPA, s. 30.1].

[138] We found that the vendor of the PARIS system (a British company by the name of In4Tek) may not access, store or transmit personal information from or to any location outside of Canada unless it is permitted by FIPPA under its contract with VCH dated February 15, 2008.

B. Stored for at Least One Year

[139] When personal information in its custody or control is used by a public body to make a decision that directly affects the individual, the personal information must be retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information [FIPPA, s. 31]. Obviously, records may need to be kept for a longer

period in accordance with other legislation, including the Hospital Act Regulation and the *Limitation Act*.

[140] We found that all records are retained in PARIS indefinitely and therefore, with respect to storage, VCH is in compliance with the one year minimum. However, the length of time that records are kept in storage raises concerns in terms of retention periods.

C. Retention Schedule

[141] In order to minimize unauthorized collection and disclosures, users should not have ongoing access to personal information that is not required for the current delivery of health services. For example, the death of a client should result in more limited access to the deceased client's health care record.

[142] Archiving of records is an effective means to minimize inappropriate access. When records are archived because they are no longer needed on a regular basis they are securely stored in a different place from active records. Access is strictly limited to health records technicians and on special request where there is a specific need-to-know.

[143] We found that there is no archiving of records in PARIS.

[144] With respect to retention of records, we found that:

- There is currently no process in place to determine retention periods for health records in PARIS.
- Since 1996, MoHS has issued five requests to health authorities requesting the preservation of records relating to patients who may have contracted hepatitis C through blood transfusions, as well as records relating to ongoing tobacco litigation.
- An initial directive to health authorities in October 1996 requested them to retain all hospital records indefinitely because of litigation regarding tainted blood. This directive was reinforced by letters in 1997 and 2000.
- MoHS issued another directive in October 2003 requesting health authorities to retain inpatient and outpatient records potentially relevant to litigation to recover health care costs related to tobacco use. This was reinforced by letter in 2007.

Recommendation 12

Records in PARIS that are no longer required for the delivery of health services should be archived on a regular and ongoing basis. A classification scheme to identify those records should be developed. Access to archived records should be strictly limited.

Recommendation 13

A records retention policy should be developed and implemented for PARIS. VCH should distinguish between information collected for administrative purposes and that collected for the delivery of health care. Administrative records not related to tainted blood or tobacco use litigation such as financial eligibility information or immigration status should be subject to a shorter retention period.

We have been told by VCH that a new Records Retention Advisory Committee will be responsible for developing a record retention policy for all VCH electronic health record systems, including PARIS. It includes representation from the Information Privacy Office. To date, it has met only once and is challenged by little or no resources to develop a health records system for eHealth.

A records retention review was completed by VCH Health Records and Transcription Services in July 2009 suggesting that there is a possibility that community care records could be destroyed depending whether they are considered as outpatient records.

A new records management bulletin was issued by MoHS in October 2009 clarifying that certain types of records are not relevant to the tobacco litigation and need not be preserved by government beyond their legislatively approved retention period, nor by health authorities beyond their operational requirements. Essentially, health authority records created after regionalization are not relevant and may be destroyed.

6. Access to Information Rights

[145] Individuals have a right of access to records in the custody or under the control of a public body, including records that contain their personal information [FIPPA, s. 4]. This right of access is subject to specified exceptions, including where the disclosure could be harmful to individual or public safety or where it would be an unreasonable invasion of a third party's personal privacy [FIPPA, Division 2].

[146] We found that:

- An access request form is available on the VCH website.
- Approximately 600 access requests were processed for PARIS clients from April 1, 2008 to March 31, 2009.
- There are routine releases of discharge summaries if clients ask for them.
- In response to access requests, VCH provides copies of paper records and copies from PARIS if they are not already printed as paper records.

- Clients do not currently receive a copy of audit logs automatically.
- Access to audit logs is new and currently under discussion.
- Concerns have been expressed by staff about disclosure of their information as users.

[147] In our view, the information that is provided to clients about their right to make access requests is inadequate in that it does not inform them about the process for making access requests, the possible scope of the request (*e.g.* audit logs), timelines, fees and where the request must be made. Improvements are needed to better inform clients about their access rights under FIPPA. With respect to an electronic health record system, clients should have access to the audit logs for their health record so that they are able to monitor disclosure of their own personal information.

Recommendation 14

Comprehensive information regarding the process for making access requests should be made available to clients.

Clients should have access to the audit logs for their health record on request, subject to any permitted exceptions under FIPPA.

We understand that work is already underway to better inform clients about access requests. A new pamphlet and newsletter provided on April 30, 2009 include the following information:

- *How to make an access request*
- *How long it will take to obtain copies of requested portions of a health record*
- *How to request corrections to the information in a health record*
- *Whether there is a charge for a copy of a health record*
- *Contact information*

We understand that this information is being included in new web pages that are in the process of being finalized.

Part III - Privacy Management Framework

[148] A privacy management framework is essential to ensure compliance with the requirements of FIPPA and good privacy practices. With respect to PARIS, our review of its privacy management framework is a holistic consideration of the structures, policies, systems and procedures in place within VCH to coordinate privacy work, manage privacy risks and ensure compliance with FIPPA. A privacy management framework reflects privacy principles and best practices and is required by the guidance document of the Canadian Institute of Chartered Accountants, *Generally Accepted Privacy Principles*.[28]

[149] Our review criteria are adapted from those that were applied by the Office of the Privacy Commissioner of Canada in a comprehensive audit that it conducted of the privacy management frameworks of four federal institutions. The Privacy Commissioner of Canada issued a report of her findings and recommendations of this audit last year. [29]

A. Governance and Accountability

i. Roles and Responsibilities

[150] An essential component of an effective governance and accountability framework for privacy is that the roles and responsibilities for the handling and management of personal information are defined and assigned, communicated throughout the organization and incorporated into the institution's control regime.

[151] The appointed head of VCH for the purposes of exercising decision-making and powers under FIPPA is the Chief Executive Officer. These powers are delegated to the Senior Executive Team. Since May 31, 2009 the roles of Chief Privacy Officer and General Legal Counsel have been combined. That position oversees both Legal Services and an Information Privacy Office ("IPO"). Her responsibilities are to:

- provide legal advice to VCH;
- advise program areas related to privacy;
- oversee and provide direction for the IPO; and
- advise on e-health audit and compliance projects as well as legislative changes.

[152] The Chief Privacy Officer reports to the Chief Financial Officer who is a member of the Senior Executive Team. As a matter of course, she reports quarterly to the Senior Executive Team on privacy matters, audit and breach

[28] Generally Accepted Privacy Principles, Exposure Draft, March 13, 2009.

[29] *Privacy Management Frameworks of Selected Federal Institutions*, Privacy Commissioner of Canada, February 2009. Former Information and Privacy Commissioner David Loukidelis was a member of the external advisory committee for the conduct of that audit.

investigations. All significant breach investigations are reported immediately to the Senior Executive Team, and if necessary, to the Board.

[153] VCH Legal Services and the IPO are responsible for:

- maintaining and administering the Information Privacy and Confidentiality Policy of VCH;
- providing privacy support services and general oversight of privacy practices within VCH, including in respect of PARIS and other electronic health care systems, to enable compliance with FIPPA;
- promoting good privacy practices throughout the organization, including legal services, education program, policies and compliance tools;
- investigating potential and actual privacy breaches brought to its attention and reporting breaches in accordance with VCH breach policies; and
- maintaining reactive and proactive privacy audit programs for core electronic health records systems in accordance with VCH audit policies.[30]

[154] The IPO is comprised of the following staff members:

- Assistant Legal Counsel (Privacy) – supports General Legal Counsel on the legal aspects of the privacy programs.
- Senior Information Privacy Officer – manages the privacy education program, advises staff on privacy matters to meet legal, ethical and trust obligations to protect personal information and investigates privacy breaches.
- Information Privacy Officer (Compliance) – manages the compliance program, including coordinating privacy impact assessments, assisting with the audit program and investigation of privacy breaches.

[155] The IPO also works closely with Vancouver Community Director, Risk Management and Client Relations and the PARIS Technical Application Lead.

[156] The Information Management / IT office is responsible for the security of the PARIS system.

[157] The Chief Privacy Officer and staff of the IPO are members of internal committees responsible for the management of PARIS and eHealth generally within VCH, including the following:

- The PARIS Privacy, Security, Confidentiality User Group is comprised of managers of program areas, as well as representatives of health records, risk management, security services and the technical application lead. The Group

[30] Information Privacy and Confidentiality, Vancouver Coastal Health, 10-Sep-2006, revised 11-Sep-2008.

is chaired by the Senior Information Privacy Officer of the IPO and reports to the PARIS Steering Committee.

- The PARIS Steering Committee is comprised of directors of program areas, General Legal Counsel, senior security representatives and the Technical Application Lead.
- The VCH/PHC iEHR Steering Committee reports to the Chief Executive Officer.
- IMIS Integrated eHealth Committee was recently established to create a vision and develop a plan for eHealth in VCH and Providence Health Care. It reports to the VCH Senior Executive Team through the Chief Information Officer with input from the VCH IMIS Strategy Council. It is comprised of Senior Executive of VCH and Medical Representatives.
- The Records Retention Advisory Committee is a new committee that includes IPO representation. (See Recommendation 17.)

[158] In terms of roles and responsibilities in relation to privacy within VCH, we found that:

- Combining the roles of General Legal Counsel and Chief Privacy Officer helps to ensure that privacy is an organizational priority at VCH.
- The governance structure and reporting relationships of staff responsible for privacy are appropriate.
- Participation of the Chief Privacy Officer and IPO staff in policy- and decision-making processes within VCH is appropriate.

ii. Privacy Outputs

[159] Another essential component of a privacy framework is that an individual or body of senior personnel within the public body defines and documents privacy policies, oversees compliance with them and ensures effective and timely decision-making with respect to privacy outputs such as privacy impact assessments ("PIAs").

[160] We found that:

- The Chief Privacy Officer sets privacy policies with the support of the Chief Financial Officer who is a member of the Senior Executive Team.
- The following privacy policies are in place:
  - Information Privacy and Confidentiality (Sept 10, 2006);
  - Management of Information Privacy Incidents (Aug 1, 2006); and
  - Reporting Theft or Loss of Information or Information Storage Device (June 26, 2006).

The following additional privacy policies were recently developed as a result of this review:

- *Auditing Access to Electronic Health Records (Jan 6, 2009),*
- *Printing of Electronic Health Records (June 5, 2009),*
- *Role-based Access Control (June 5, 2009),*
- *Access Administration (June 5, 2009), and*
- *Guidelines on Collection of Personal Information (Sept 20, 2009).*

[161] A public body must perform comprehensive PIAs to enable it to properly assess whether a proposed system, program, policy or legislation has any privacy impacts and complies with FIPPA.

[162] A public body should perform a PIA, in consultation with its privacy experts, at the conceptual phase of each proposed system, program, policy or piece of legislation. The PIA should be performed early in order to guide the decision on whether to proceed at all in light of any adverse privacy impact or concerns about compliance with FIPPA. The completed PIA should, in cases where the public body decides any privacy impact can be mitigated if it proceeds, be used to design the program, policy or legislation in a way that mitigates any privacy impact as much as possible. Subsequent PIAs should also be completed at the design and implementation phases to ensure an appropriate privacy framework is put in place.

[163] We found that:

- The Chief Privacy Officer is responsible for completing PIAs for PARIS.
- There was an initial PIA for PARIS completed in 2002 that was last updated in 2007.
- A second PIA was completed for PARIS dated 2005.
- Both PIAs identify a number of outstanding privacy issues and concerns and make policy recommendations.

B. Systems and Practices to Ensure Compliance and Performance Monitoring

[164] Compliance with FIPPA obligations must be supported by effective compliance and performance monitoring on an ongoing basis.

[165] An important indication of this is whether the organization establishes annual and multi-year privacy performance plans, targets, and measures, and reports on results.

i. Privacy Performance Plans

[166] The Chief Privacy Officer develops a privacy performance plan each fiscal year. The purpose of the plan is stated as follows:

> This plan sets out the strategic direction and goals of the Information Privacy Office (IPO) and what we plan to achieve over the 2008-9 financial year. By fulfilling our strategies and plans, we hope to make a difference to privacy awareness and compliance within our organization. Our goals for this year reflect VCH's commitment to continue to enhance privacy measures to protect personal information under our stewardship. We aim to encourage good privacy practice to meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

[167] This plan is an internal plan of the IPO only. There is no approval process. The IPO produces a "performance tracking" document to track the status of its goals.

[168] There is no multi-year plan.

Recommendation 15

VCH should establish annual and multi-year privacy performance plans, targets, and measures, and report on results.

ii. Ongoing Monitoring, Assessment and Adaptation

[169] In order for a public body to be FIPPA compliant, it must monitor, assess and adapt its privacy policies, procedures and practices on an ongoing and as-needed basis.

[170] In our review of the activities of the IPO, we found that:

- Every policy that is passed has a revisit date of six months, one year, or two years depending on the type of policy.
- Policies are also revisited in the interim if there is a legislative change or system change.

iii. Resources

[171] It is essential that a public body assign resources to ensure that it can effectively and efficiently discharge its obligations under FIPPA. Evidence of an adequate level of privacy resources includes the following activities:

- PIAs are updated as required,
- Changes in privacy policies are communicated to staff,
- System is in place for capturing privacy breaches to ensure they are identified, reported and remedied,
- Documented privacy incident and breach management program has been implemented.

PIA is updated as required

[172] As previously mentioned, a PIA should be completed at the conceptual, design and implementation of an electronic health record system. Once the system has been operationalized, the implementation PIA should be reviewed on a regular basis and updated as required. At a minimum, it should be updated whenever there is a material change to the system.

[173] We found that:

- VCH acknowledges that the most recent implementation PIA for PARIS is out of date.
- There is a process that prompts outstanding issues in the PIA.
- Policy responses to all recommendations in the most recent implementation PIA are under development or there are structures in place.

Recommendation 16

The implementation PIA for PARIS should be treated as an evergreen document that is reviewed and updated on a regular basis as required.

Changes in privacy policies are communicated to staff

[174] We found that:

- Changes in privacy policies are communicated to VCH staff by the IPO via email and the VCH intranet site.
- Memos, guidelines and brochures regarding staff privacy obligations are regularly distributed to staff by the IPO and are accessible on the VCH intranet site.
- A quarterly update entitled “Privacymatters” is distributed to managers and directors to advise them of privacy initiatives.
- The PARIS website has a privacy page and a link to the IPO site.

System is in place for capturing privacy breaches to ensure they are identified, reported and remedied

[175] VCH does reactive audits in response to a complaint of a privacy breach. There has also been a proactive audit program in place at VCH since November 2008.

[176] In our review, we found that:

- Audit log data collected from seven core electronic information systems at VCH are stored in one integrated database.
- Proactive queries are run against the data, including:
  - same surname look up,
  - volume reports,
  - clients accessed the most by the most users, and
  - Enhanced Information Security Clients ("EIS").
- There is one monthly report of the results.
- There are two PARIS-specific audits since December 08:
  - EIS NOT ON TEAM report will identify access to a client's record where the client has been flagged as EIS and the user that has accessed them is not on the client's team.
  - PARIS NOT ON TEAM report will indicate access to a client's record where the user is not a member of the client's treatment team.
- For the PARIS-specific audits, the former is always investigated and happens rarely; the latter produces such a large volume of reports that the data is not analyzed and is thus currently ineffective.

[177] If a breach is suspected based on audit results, IPO sends a breach form by inter-office mail to the manager of the program area where the breach occurred. The onus is on the manager to investigate and to make a decision on how to deal with the breach in conjunction with Employee Engagement (*i.e.* Human Resources). Possible responses to an investigation are:

- Deemed appropriate
- No action required
- Education
- Caution
- Note to file
- Termination
- Report to professional regulatory body

[178] IPO will follow up with the manager if there are frequent breaches in the same area or escalate the matter if there has been no response after six weeks.

[179] IPO developed guidelines with respect to penalties for a privacy breach to try and ensure there would be a consistent approach across VCH.

[180] It is anticipated that the ability to conduct proactive audits on the PARIS system could improve considerably once the role-based access model and restricted caseload is in place. At present, there is so much access to client records that it is impossible to analyze the reports. In future, because there will be fewer users granted permission to access an individual's records, there will be a fewer number of users that are flagged and thus more effective auditing capability.

Recommendation 17

The conduct of a pro-active audit of access by users to client records (currently known as PARIS NOT ON TEAM) must be changed to reflect the new role-based access model based on clinical relationship and restricted caseload (see Recommendation 5).

Documented privacy incident and breach management program has been implemented

[181] The IPO has a privacy incident and breach management program. Incidents and privacy breaches are managed, recorded and reported. Some of the tools employed in the process include the following:

- IPO hotline – included on all IPO communications and media. Messages are checked several times a day; this is a shared responsibility among the privacy officers.
- IPO direct email – address included on all IPO communications and media. Messages are checked several times a day; this is a shared responsibility among the privacy officers.
- IPO tracks all privacy queries, incidents, and breach investigations in a centralized database called "PRIMO". It is located on a secured fileshare only accessible to members of the IPO. "PRIMO" forms the basis for the reporting structure and has the ability to communicate statistics on all categories, summaries and resolutions.

iv. Privacy Education and Training

[182] In-depth and ongoing privacy education and training for all employees of a public body who have access to personal information is necessary to ensure compliance with privacy obligations.

[183] In our review of privacy training and education at VCH, we found that:

- Since March 2008, a 20 minute online privacy tutorial created by the IPO is available to staff on the VCH intranet site,
- New staff are informed about the online privacy tutorial at their orientation session and its completion by new staff is tracked,
- There is no requirement for existing staff to take the tutorial,
- There is no mandatory ongoing training and education about privacy,
- All PARIS users are required to take two days of training that includes limited privacy training, including distribution and discussion of the information and privacy policy, and
- IPO staff give presentations about privacy obligations to staff on an ad hoc basis.

[184] In our view, privacy training and education at VCH is inadequate. The online privacy tutorial is useful but it is not mandatory for existing staff, is generic in nature and does not include specific information about the privacy and security framework for electronic information systems (*e.g.* role-based access model). There should be more practical hands-on privacy training for PARIS users. Despite these shortcomings, we also found that there is a commitment to continuous improvement with respect to privacy in the IPO and a slow shift towards a culture of privacy within VCH. Building on these strengths, VCH should develop specific modules on privacy issues related to electronic health record systems and institute mandatory requirements for privacy training on an annual basis.

Recommendation 18

Staff should be required to complete privacy training each year that includes completion of a comprehensive privacy tutorial with specific modules on privacy issues related to electronic information systems. Completion of this training should be tracked and linked to an annual renewal of user privileges.

Confidentiality agreements

[185] We found that:

- Staff sign confidentiality undertakings once only.

- Confidentiality undertakings are signed in paper and kept on file.

[186] In our view, staff should sign confidentiality undertakings on an annual basis on the completion of the refresher course. This would serve as an important reminder to staff of their privacy obligations and reinforce messaging around VCH's expectation of an ongoing commitment to protect the privacy of clients. A new software program is likely to be required to document undertakings signed by all users on an annual basis.

Recommendation 19

The PARIS confidentiality undertaking form should be revised to reflect the "need-to-know" access model based on clinical relationship. This should be done as soon as the new access model is in place (see Recommendation 5).

Recommendation 20

Staff should sign confidentiality undertakings on an annual basis.

Conclusion

[187] The protection of privacy with respect to health care information is critical to the health and dignity of each patient, as well as the foundation of the trust relationship between patient and health care provider. The importance of ensuring that health care information be collected, used and disclosed only to appropriate health care providers and be protected from outside threats cannot be overstated. We found the PARIS system seriously deficient in these regards. It must be noted that many of the problems were not caused by PARIS, but instead were the result of human decisions in respect of how personal health information would be collected into, made available by and disclosed through the system, which is a human issue.

[188] Principal among these deficiencies is an overly generous workgroup-based access control model that should be reconfigured to role-based access to better control and limit the access users have to very sensitive personal health information.

[189] The security of the PARIS system in terms of protecting personal health information was woefully inadequate but has been improved by VCH's response to the Auditor General's recent findings with respect to the security of the system. In addition to implementing the security recommendations of the Auditor General, we recommend that VCH ensure that core security standards be addressed,

including documenting change control procedures, implementing controls to detect, prevent and log unauthorized data exchanges and encrypting data both during transmission and storage.

[190] We found that VCH is routinely, and without legislative authority, disclosing identifiable data sets to other public and not-for-profit entities, including the Ministry of Health Services and the Canadian Institute for Health Information. We strongly recommend this practice cease or, in the alternative, that VCH provide de-identified information only. The lack of authority for these external disclosures of personal information outside VCH is particularly troubling given that the appropriate remedy to legalize these disclosures is already in place—designation as a health information bank under the E-Health Act.

[191] Overall, we found that VCH had in place a good privacy management framework. Unfortunately, the main components of this framework were developed after PARIS was implemented in community programs at VCH. Recent initiatives such as combining the role of general legal counsel and chief privacy officer, developing new privacy policies and requiring privacy training for new staff, are all positive achievements. However, further implementation of privacy policies and other specific measures such as an evergreen PIA are necessary in relation to PARIS. Clearly, a stronger, more coherent and integrated privacy lens must be applied to the administration and security of PARIS. In our view, the Chief Privacy Officer should liaise more closely with IT system administration at VCH in order to ensure that an adequate privacy and security framework is implemented in PARIS and other electronic health record systems at VCH.

[192] VCH has been cooperative throughout this investigation, and has pro-actively taken steps to remedy some of the problems we uncovered during the course of our investigation and we thank them for that.

[193] Over the next year, we will continue to monitor the implementation of our recommendations. We also anticipate that these recommendations will influence the development of other eHealth systems in the Province and that patient privacy will be protected to the extent required by provincial statute and the common law.

March 5, 2010

ORIGINAL SIGNED BY

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

OIPC File No.: F07-31670

SUMMARY OF RECOMMENDATIONS

PART II - Compliance with the *Freedom of Information and Protection of Privacy Act*

Recommendation 1

VCH should not collect personal information regarding delivery of health care to an associated person unless it is necessary for the delivery of health care to a client and only the minimum amount of personal information is collected.

Recommendation 2

VCH should stop indirectly collecting personal information from the Enterprise Master Patient Index without authority to do so.

Recommendation 3

VCH should develop more comprehensive web pages and notices for its clients regarding the collection, use and disclosure of personal information through PARIS. At a minimum, they should include a brief explanation of PARIS, the access model within VCH and the disclosures outside VCH.

Recommendation 4

A new, more granular, role-based access model for PARIS should be developed and implemented.

This model would include a comprehensive roles matrix that maps job functions with the personal information and privileges required to perform those functions. Roles should be defined at the highest level of specificity and granularity as possible, while still taking into account business and clinical workflows within program areas. The amount of personal information within the various modules should also be reviewed so that, in accordance with the least privilege principle, each role only has access to the minimum amount of personal information necessary to perform their functions.

The role-based access matrix must be fully documented and regularly checked and updated by the Information Privacy Office and IT system administration.

Recommendation 5

Roles should be further limited to client relationship.

The functionality that exists in PARIS for client allocation should be deployed to the maximum extent possible. We were advised that there may be some

challenges where there is a shared model of care and services are provided on a 24 hour basis. In that case, consideration may be given to restrictions based on location with an attestation of clinical relationship.

Recommendation 6

Users should be assigned to roles by a central body within VCH with privacy expertise so that the need-to-know and least privilege principles are applied consistently.

Recommendation 7

VCH should discontinue disclosing personal information to MoHS and the Canadian Institute for Health Information from PARIS that is not authorized under FIPPA. Only de-identified information should be disclosed to:

- MoHS for the purposes of health system and program planning, monitoring program and system performance and reporting on service activities; and
- the Canadian Institute for Health Information for the purposes of health research and statistical analysis.

Personal information should only be disclosed to health care providers at Providence Health Care with consent.

Recommendation 8

VCH should ensure that all information-sharing agreements require recipients of personal health information outside VCH to maintain specific reasonable standards of privacy and security protection.

Recommendation 9

VCH should develop a comprehensive secondary use policy to ensure that the provisions in s. 35 of FIPPA are met. This policy should include requirements for security and confidentiality and a template for research agreements

Recommendation 10

All individuals should be advised of and have the option to be considered as EIS without having to justify their choice. Individuals should be consistently informed of the option to be flagged as EIS, its implications and how this option is exercised.

Recommendation 11

There should be a clear and more expansive notice to clients on the VCH website and elsewhere about the EIS option. This notice should describe the access model in PARIS and indicate the availability of the EIS option, the process for clients seeking to be flagged as EIS and the implications of being flagged. Clients should also be informed that clinical advice is available if they are considering this option.

Recommendation 12

Records in PARIS that are no longer required for the delivery of health services should be archived on a regular and ongoing basis. A classification scheme to identify those records should be developed. Access to archived records should be strictly limited.

Recommendation 13

A records retention policy should be developed and implemented for PARIS. VCH should distinguish between information collected for administrative purposes and that collected for the delivery of health care. Administrative records not related to tainted blood or tobacco use litigation, such as financial eligibility information or immigration status, should be subject to a shorter retention period.

Recommendation 14

Comprehensive information regarding the process for making access requests should be made available to clients.

Clients should have access to the audit logs for their health record on request, subject to any permitted exceptions under FIPPA.

Part III - Privacy Management Framework

Recommendation 15

VCH should establish annual and multi-year privacy performance plans, targets, and measures, and report on results.

Recommendation 16

The implementation PIA for PARIS should be treated as an evergreen document that is reviewed and updated on a regular basis as required.

Recommendation 17

The conduct of a pro-active audit of access by users to client records (currently known as PARIS NOT ON TEAM) must be changed to reflect the new role-based access model based on clinical relationship and restricted caseload (see Recommendation 5).

Recommendation 18

Staff should be required to complete privacy training each year that includes completion of a comprehensive privacy tutorial with specific modules on privacy issues related to electronic information systems. Completion of this training should be tracked and linked to an annual renewal of user privileges.

Recommendation 19

The PARIS confidentiality undertaking form should be revised to reflect the "need-to-know" access model based on clinical relationship. This should be done as soon as the new access model is in place (see Recommendation 5).

Recommendation 20

Staff should sign confidentiality undertakings on an annual basis.

Erratum

The originally published version of this report stated at para 151 that VCH had delegated the powers of the Head to its Chief Privacy Officer. This statement was factually incorrect and has been amended

Appendix A

Glossary[31]

Access – disclosure of personal information by the provision of access to personal information [FIPPA, Schedule 1]

Archiving - a systematic approach to storing and protecting data that is no longer needed

Audit log - a chronological record of access to data in an electronic database that typically includes user ID, time of access, resources that were accessed, device used to access the information and modifications that were made

Classification - a system for determining the sensitivity of personal information and for establishing priorities for information security and privacy protection

Collect - to gather, obtain access to, acquire, receive or obtain personal information either directly from an individual or indirectly

Collection (direct) - gathered from the individual to whom the information relates

Collection (indirect) - gathered from any source other than from the individual to whom the information relates

Compliance - meeting requirements as set out in relevant laws, regulations, standards, ethical principles, codes of conduct, contractual agreements or policies and procedures

Confidentiality - information is not made available or disclosed to unauthorized individuals, entities or processes

Consent - voluntary agreement by an individual, or his or her legally authorized representative, to allow the collection, use or disclosure of the individual's personal information

Control (of a record) - the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure

Custody (of a record) - having physical possession of a record, even though the public body may not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and security

Data - pieces of information such as individual facts or results

[31] Definitions adapted from: *Guidelines for the Protection of Health Information – December 15, 2006*, COACH: Canada's Health Informatics Association*; CIHR Best Practices for Protecting Privacy in Health Research,* September 2005; International Organization for Standardization 7498-2: 1989; Information Management and Information Technology Management section of the Core Policy and Procedures Manual of the BC Government; and *Pan-Canadian Health Information Privacy and Confidentiality Framework,* Health and the Information Highway Division, Health Canada, January 27, 2005. Where noted as "FIPPA, Schedule 1", the definitions are from the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165.

De-identified information - personal information that has been modified so that the identity of the subject individual cannot be determined by a reasonably foreseeable method. This involves the removal of name and address, if present; and removal or encryption of identifying numbers, such as personal health number and chart number

Disclosure - to release or make available personal information to a person, other than the person the information concerns

Electronic health record - an electronic record containing personal information that is stored for the purpose of delivering health services that may be accessed on a frequent and regular basis by authorized users with access privileges

Encryption - the process of mathematically converting information so as to render it unintelligible without a key to decode it

Firewall - a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks

Least privilege - a security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Masking - a process of restricting access to personal information by making the information in a record visible only to certain users

Need-to-know - a privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office

Personal information - Recorded information about an identifiable individual other than contact information [FIPPA, Schedule 1]

Privacy - in relation to information, privacy involves the right of individuals to determine when, how and to what extent they share information about themselves with others

Privacy breach - occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information

Privacy Impact Assessment (PIA) - a tool used to assess the possible privacy-related consequences of proposed systems and practices for the collection, use and disclosure of personal information. For example, a PIA is required at the three stages of an electronic health record system: conceptual, design, and implementation and should be revised whenever there is a material change to the system

Record - includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records [FIPPA, Schedule 1]

Retention - the process of holding data or information in a secure or intact manner usually for a defined period of time after which it may be permanently destroyed

Role-based access control - a policy and technology architecture involving the assignment of permissions to roles that are determined by the amount and type of information that is needed to perform the job functions of users

Security (of personal information) - security is the process of protecting personal information by assessing threats and risks to that information and implementing the procedures and systems to maintain the integrity of that information and to prevent unauthorized access, use, disclosure and disposal of that information

Service provider - a person retained under a contract to perform services for a public body [FIPPA, Schedule 1]

Sensitivity (of personal information) - the sensitivity of personal information is related to the potential for harm or stigma that might attach to the identification of an individual because of the nature of the information

Use, primary - the use of personal information for the purpose of providing individual care and administrative functions directly related to that care

Use, secondary - the use of personal information for purposes other than direct individual care and administrative functions directly related to that care. Secondary uses include planning, monitoring, research or disclosure as required by law

User - any individual who has access privileges to an electronic health record system

Appendix B

Health Information Legislation in BC

BC has a unique legislative framework governing personal information that is collected, used and disclosed for the purpose of delivering health care services. Unlike other provinces that have instituted stand-alone health information statutes (including Ontario, Alberta, and Saskatchewan), in BC there are several different pieces of legislation that apply to data flows of personal health information. In addition to the laws of general application (the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*) that apply to personal information in the custody or control of either public bodies (such as health authorities) or organizations (such as labs or physicians' offices), there are other provisions that apply to specific types of health information.

These statutory provisions are the following:

E-Health (Personal Health Information Access and Protection of Privacy) Act

This Act governs the collection, use and disclosure of personal health information through electronic databases of the Ministry of Health Services and health authorities that have been designated by the Minister as "health information banks". To date, the Act has only been applied to the new repository of lab data that is being built by the Ministry as part of a provincial Electronic Health Records system (the Provincial Laboratory Information Solution).

Pharmacy Operations and Drug Scheduling Act, ss. 12 to 16

Sections 12 to 16 of this Act govern the collection, use and disclosure of personal information through PharmaNet. PharmaNet is a provincial database of the Ministry of Health Services that is used by pharmacists in the dispensing of all prescription medication in BC.

Medicare Protection Act, s. 49

Section 49 of the Act governs the collection, use and disclosure of personal information by the Ministry of Health Services in relation to the Medical Services Plan.

Public Health Act

Health Act Communicable Disease Regulation

Specific provisions in this legislation govern the collection, use and disclosure of personal information related to public health matters, including mandatory reporting of infectious diseases or health hazards. Section 9 of the *Public Health*

Act permits the same health-related purposes for collection, use and disclosure as are permitted in the E-Health Act.

Continuing Care Act, s. 5

Section 5 (as amended) authorizes the Ministry of Health Services and a health authority to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

Hospital Insurance Act, s. 7

Section 7 authorizes the Ministry of Health Services or a hospital to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.