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

INVESTIGATION REPORT F06-02

INVESTIGATION INTO SECURITY OF PERSONAL INFORMATION HELD BY VANCOUVER COASTAL HEALTH AUTHORITY'S EMPLOYEE AND FAMILY ASSISTANCE PROGRAM

June 7, 2006

Quicklaw Cite: [2006] B.C.I.P.C.D. No. 17
Document URL: www.oipc.bc.ca/investigations/reports/InvestigationReportF06-02.pdf
Office URL: www.oipc.bc.ca

TABLE OF CONTENTS

Appendices

1.0 INTRODUCTION

[1] The Employee and Family Assistance Program ("EFAP") is a confidential employee-counselling service operated as a component of the Vancouver Coastal Health Authority ("VCHA"). It is staffed by VCHA employees and is responsible to VCHA. EFAP is a program of the VCHA and is not a separate entity. As a health authority established under the *Health Authorities Act*, VCHA is a "health care body" and therefore a "public body" covered by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). EFAP's actions are therefore those of the VCHA for FIPPA purposes.

[2] Public bodies in British Columbia are under a statutory duty to protect the personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:

> **Protection of personal information**
>
> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[3] In order to ensure client confidentiality—a critical element of EFAP's work—EFAP established, as an interim measure pending the delivery of a comprehensive hardware and software security upgrade, a stand-alone computer on which to store its client database. The computer contained a great deal of personal information, much of it very sensitive, about thousands of EFAP clients. The computer was stolen from the EFAP administration office, exposing the personal information of EFAP clients to potential unauthorized disclosure or use.

[4] This report is the product of my investigation, under s. 42 of FIPPA, into the potential breach of personal privacy resulting from the theft of the computer. This report examines the adequacy of protective measures taken by EFAP under s. 30 of FIPPA. This report makes findings, and contains conclusions, but no order is made under s. 58 of FIPPA.

2.0 BACKGROUND

[5] On the afternoon of March 25, 2006, a thief broke into the EFAP office. The thief went to the nearest open office—the office of the manager of administration for EFAP—located a few steps in a straight line from the office entrance. In that office, in plain view, was a desktop computer that contained EFAP's client database. The thief disconnected the cables and made off with the computer. Cleaning staff later discovered the break-in and contacted the EFAP manager, who in turn contacted police and went to the office immediately to meet the attending officers. The officers took the details of the stolen item, including a unit identification number recorded on an inventory sticker, and offered their opinion that this theft bore the marks of a typical "smash and grab" operation.

[6] The details of the theft were relayed to the Office of the Information and Privacy Commissioner ("OIPC") by the Freedom of Information Coordinator for the VCHA on the afternoon of March 29, 2006. On the morning of March 31, 2006, a conference call was held between representatives of VCHA, EFAP, Providence Health Care (a health organization having a service agreement with EFAP) and an OIPC representative in order to conduct an initial risk assessment and review of mitigation strategies. At that time, the OIPC was informed that the stolen computer contained a database with files on approximately 11,000 EFAP clients.

[7] The Information and Privacy Commissioner directed me to investigate this matter. I attended at the EFAP office to perform a site inspection on April 6, 2006 and at that time conducted an in-depth interview with the office administrator responsible for the EFAP computer system. I was in frequent contact with VCHA staff responsible for steering VCHA through the post-theft and client notification period.

3.0 DISCUSSION

[8] **3.1 Description of EFAP**—EFAP is an operating program of VCHA that provides confidential counselling services to employees, and their family members, of several health authorities and organizations which EFAP serves—the Provincial Health Services Authority the Fraser Health Authority, Providence Healthcare, the Evergreen Baptist Care Society and several smaller groups on a contracted fee-for-service basis.

[9] EFAP staff told me that EFAP takes the confidentiality of its client information seriously. Some of the measures it takes to protect the privacy of its clients, as described in the EFAP services brochure, include:

- private waiting rooms and a separate entrance and exit;

- staggered appointment times to minimize the prospect of clients bumping into one another;
- non-identifying statistics used to report to the EFAP Board of Directors;
- electronic access restricted to within the program (the EFAP database is not networked to any outside computer system).

[10] In my interview with EFAP's manager of administration, who has been with EFAP since its inception in November of 1993, she noted the overall acceptance and success of the program, which led over the years to the opening of a branch office (with administrative functions) in Surrey, six satellite counselling offices and to services throughout the province provided by a network of fee-for-service counsellors reporting to EFAP. EFAP has an executive director, two clinical managers and an advisory board with 18 members.

[11] Over a period of fewer than 13 years, EFAP has grown from a small unit serving solely the employees of Vancouver General Hospital to an organization with more than 25 core team members and approximately 60 service providers throughout the Province, serving 60,000 employees. The largest period of growth occurred during 2002-2003. The large growth in caseload numbers in turn put pressure on EFAP's ability to maintain an electronic case-management database adequate to support the needs of the organization.

[12] **3.2 EFAP's Information Technology**—Throughout its history, EFAP chose to keep its client database in its administrative office rather than on an offsite server operated by VCHA. Several factors contributed to this decision:

1. EFAP communicates with its branch office in Surrey and with VCHA through a virtual private network ("VPN") maintained by an external service provider. Through a combination of firewalls, data encryption and user authentication, the VPN offers a secure method of transmitting information over an unsecured network (*i.e.*, the Internet). However, the VPN, due to its elaborate security structure, does not provide sufficient bandwidth for the VPN server to act as a general server for EFAP.

2. EFAP's administration manager explained that EFAP must be careful to maintain an arm's-length relationship with VCHA's information technology personnel because, as VCHA employees, those staff members might one day be clients of the EFAP counselling service.

3. As part of their job functions in a recently-expanded organization, these staff needed to access the database through a local-area network for the purpose of billing client organizations for services rendered to their employees. EFAP selected a desktop computer to hold the database of 11,000 client records for its ability to serve the needs of personnel in the administrative head office.

[13] The computer ran the Windows 2000 operating system. This system was viewed by EFAP management as offering slightly more secure access and a workable interface with the other computers in the office, making it useful as an interim server. It was configured and set up to perform as a server in the summer of 2005.

[14] Several months earlier, as part of EFAP's plan to increase the functionality of its data server by making file sharing and data backup more efficient and secure, and to create a web-based platform so that service providers could have secure access to the client database, a relatively sophisticated server was purchased and was being held in storage at VCHA. At this time, EFAP, working with a systems consultant, set about finding or developing a software solution that would meet EFAP's needs for robust security, backup features, multiple permission-based access levels and mandatory password updating.

[15] While waiting for installation of the new hardware/software solution, EFAP employees were aware of the physical vulnerability of the desktop computer and, to a lesser degree, the level of software security protecting the personal information contained on it. VCHA information technology staff gave EFAP a computer anti-theft cable that EFAP intended to use to provide a measure of physical security for its interim server. The cable had not been installed when the computer was stolen, as a suitable lock that would fit the cable had not yet been purchased.

[16] **3.3 What Personal Information was Involved?**—There were three classes of personal information involved. The first class of personal information (Class 1) was the personal information of 10 EFAP employees, whose personal information relevant to payroll management was kept in a data file. This included name, social insurance number (SIN), scanned copies of the individual's birth certificate, personal health number and a sample of a void personal cheque.

[17] The second class (Class 2) was the personal information of approximately 1,300 EFAP clients. The personal information of these clients as recorded on EFAP's intake form included name, address, date of birth, the dates of initial counselling appointments and a brief description of the presenting clients' problems. As these files were inactive for a period of two or more years, they were treated as closed files, and scanned copies of the client's clinical notes from EFAP counselling sessions were kept in a separate data file on the same hard drive, with the client being identified by the personal ID number assigned at the time of the client's initial contact with EFAP. These notes were held in EFAP's interim server pending a decision on a longer-term storage solution. The clinical notes would constitute the most sensitive personal information on the database, given that they would likely document intimate private matters that the client intended to share only with the counsellor.

[18] The third and largest class (Class 3) consisted of personal information of over 9,500 current and former employees of organizations served by EFAP who had arranged for counselling. The personal information fields in the EFAP database included name, address, date of birth, the dates of initial counselling appointments and a brief description of the presenting problems, such as depression, work-related conflict, grief, substance abuse or divorce.

[19] **3.4 What Security Measures Were in Place Before the Theft?—**The following is a summary of the security measures and risks in place or existing at the EFAP administrative office before the theft.

[20] <u>Building vulnerabilities and risks</u>: The high-rise office building housing the EFAP administrative office in Vancouver remains open on Saturdays; there are no restrictions such as passcards required to use the elevators during regular business hours including Saturdays. After-hours use is restricted. A security officer is on duty after hours and on Saturdays, and patrols the floors in a random pattern. There are security cameras recording activity at entry and exit points—except for two particular exits. EFAP staff informed me that building security staff conducted an examination of security system tapes for the time in question and found no evidence of a person leaving the building with the computer or an object of similar size.

[21] <u>Physical security of the office</u>: A floor to ceiling panel of glass to the left of the door frame provided easy entrance to the thief, who smashed the glass near the door handle, then reached in and unlocked the door. Once in the office, the thief proceeded directly to the manager's office, which was unlocked. The office did not have an alarm system.

[22] <u>Physical security of the computer</u>: The computer was not secured in a locked room or cabinet. It was not secured by a cable, metal frame or similar device. Nor was it hidden from sight.

[23] <u>Software security of the computer database</u>: The computer's operating system, Windows 2000, had only a user password as an enabled security function.

[24] The software used for the interim database had a password protection function. The password function was not, however, in use, as it would not work in conjunction with the database replication feature that EFAP used in order to maintain a working copy of the database at its other administrative office in Surrey.

[25] Information on the computer was not encrypted. Data could be viewed directly by anyone who bypasses the Windows user password.

[26] The VPN (described in section 3.2 above) was not used to hold client files, so it is not relevant to the security of client data. It was and is, however, used to

securely transmit relatively low volumes of client information between EFAP offices as necessary for EFAP to provide client services.

[27] A backup copy of the database was held on another computer ("snap server"). This enabled the continuation of the office's work and provided the basis for EFAP to attempt to notify its clients of the loss of their personal information.

[28] **3.5 Policies and Procedures**—EFAP did have a general written policy regarding confidentiality of client information. However, at the date of the theft, EFAP had no specific policies or procedures in place that were designed to minimize the possibility of physical intrusion or data theft. Staff understood they had a general duty to protect client confidentiality and to take common-sense precautions, such as locking the main entrance door after business hours or when leaving the office at the end of the day.

[29] EFAP staff, as employees of VCHA, are bound to observe VCHA policies and procedures for the protection of personal information. VCHA says it provides periodic educational seminars for its staff on FIPPA obligations, office security and related matters, in addition to issuing bulletins on privacy requirements and good practices. However, as at March 25, 2006, VCHA had no written policies in place, applicable throughout the organization, addressing the issue of security standards and procedures for computer hardware and data. Such a policy would be binding on all personnel responsible for the planning, execution and monitoring of data security throughout this decentralized organization. The absence of such an important policy is not acceptable and should be remedied.

[30] Staff at EFAP and other parts of VCHA consistently stated to me that EFAP has generally operated at arm's-length from VCHA due to the sensitivity of the records maintained by EFAP, as a counselling organization, concerning VCHA employees. VCHA acknowledges that EFAP has traditionally exercised considerable independence in maintaining and operating its data storage equipment. This resulted in a situation in which it is apparent that EFAP was not subject to security audits or similar procedures that might otherwise have been conducted by VCHA information technology or security personnel. Thus, EFAP was in a position of being, from a practical perspective, on its own.

[31] **3.6 Analysis of Data Sensitivity and Protective Measures**—Section 30 of FIPPA requires public bodies to take reasonable measures to protect information under their custody or control. In Investigation Report F06-01,[1] Commissioner Loukidelis said this about s. 30:

> [49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on

[1] http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf.

> 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.

[32] The reasonableness of security measures will depend on the sensitivity of the information. As the Commissioner 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.

[33] As noted earlier, EFAP held personal information in the stolen computer pertaining to approximately 11,000 individuals. The information held in the database can be divided into three classes, as set out above. Each class of information reflects a different sensitivity level with respect to the potential impact on the individual data subject resulting from the breach. I refer to each class of data in the analysis that follows.

[34] Class 1: The information held on the 10 EFAP employees included the SIN. The SIN is a useful piece of information for those intent on identity theft because it can be used as the starting point for replicating a series of identification cards, particularly if the identity thief is also able to obtain the individual's birth date, as he would have in this case, with birth certificate and personal health number also forming part of the file. Such information would greatly facilitate the process of replicating an individual's identity and of obtaining credit cards or opening bank accounts and obtaining personal loans.

[35] Class 2: The 1,300 clients who had clinical notes stored on the server as Adobe portable document format records were at risk of harm in the event of a breach. Each clinical note file would conceivably highlight individual vulnerabilities relative to the nature of the problem for which the client sought counselling. Disclosure of this information could cause hurt feelings or

embarrassment at the very least and at worst could be a source of fear, despair or psychological harm.

[36] Even if the data are never accessed, the client may still suffer stress or anxiety over the possibility of the data being made public. In the economic sphere, this information could possibly be used as a basis for targeting for identity theft or other forms of fraud against the client. This consequence, while inherently indeterminate, was nonetheless reasonably foreseeable, had a data risk analysis been performed as part of a security planning and design exercise.

[37] Class 3: The remaining clients, who number in excess of 9,500, had basic contact information on file—name, address, telephone number, employer—in addition to more sensitive information in summary form pertaining to the issues about which the client was seeking counselling. These clients would, in the same manner as clients with Class 2 information, be vulnerable to personal hurt or embarrassment from disclosure, and mental stress or anxiety over the possibility of disclosure. For these clients, the economically valuable information available to a fraudster would be less detailed, but could nonetheless be used as the starting point for identity theft.

[38] The security of the personal information rested on two factors: physical security of the office environment; and the computer installation and software security, that is, the protection against access to the information in the event of an unauthorized individual gaining control or possession of the computer. I will review the two forms of security separately.

Physical security

[39] Physical office security was inadequate. The glass panel beside the door provided no real protection against forced entry. Reinforced glass or an equivalent entry-resistant polycarbonate material would have been appropriate for this application, along with a reinforcement plate in the area of the handle and latch to render the door more resistant to forced entry.

[40] Individual offices containing personal information, whether in paper records or computer hardware, were not locked. The latch and lock mechanism should be more than symbolic—the door should be reasonably resistant to forced entry.

[41] Computer hardware containing personal information was not physically secured against removal. Servers and other computers holding sensitive personal information in the hard drive (as opposed to "dumb terminals" that do not store data) should be locked securely against physical removal by a cable designed for the task or locked within a cabinet or similar structure capable of resisting removal of the computer. Any computer performing a central data storage or server function should be kept in a highly secure cabinet or room with a superior resistance to forced entry.

Software security

[42] EFAP software security measures designed to prevent unauthorized access to personal information were minimal, since the data on the computer were protected only by an operating system log-in user name and password.

[43] An operating system log-in (password and user name) is known to be a security measure bypassed with sufficient ease that it should not be the only means of protecting sensitive personal information. Instructions for bypassing the operating system are available on the system itself and on the Internet. Additional security measures are built into and can be enabled in the operating system, but these were not implemented.

[44] Once a computer has fallen into the hands of an unauthorized individual, the only reliable safeguard standing between that individual and the personal information on a client database such as that involved here is encryption, which is the coding of the information into unintelligible data by means of a mathematical algorithm. Only the holder of the encryption decoding key can gain access to usable information. This was once an expensive and difficult process to implement, but that is no longer true with the advent of inexpensive and user-friendly encryption programs.

[45] As noted in Investigation Report F06-01, passwords do not constitute encryption.[2] While robust encryption programs are so difficult as to be essentially impossible to defeat, the same cannot be said for passwords, which password generator programs can and do overcome. This is not to say that passwords are not useful, as they will deter many unauthorized users from pursuing data.

[46] EFAP's manager of administration was aware of the physical vulnerabilities of the system, but less aware of the inherent weakness of password protection as a means of data security, as discussed below. It is apparent that EFAP was working toward installation of a system that would offer better data protection and physical security. EFAP had hoped and believed that migrating to a new server would be a far quicker process than what in fact transpired. The unfortunate reality is that, in the meantime, EFAP client information was not protected by reasonable security measures, given its sensitivity and the relative ease with which the information could have been secured.

[47] Following the computer theft, EFAP commissioned a technical risk analysis report from a reputable consulting firm. The analysis included an assessment of the ease with which information on the stolen computer could be accessed. The risk analysis report essentially confirmed the inadequacy of data security measures and found that the data could be accessed by anyone with the

[2] See footnote 21, Investigation Report F06-01.

level of technical knowledge of a hobbyist home computer user. The report recommended that EFAP adopt standard information technology security practices in the form of ISO 17799 (Code of Practice for Information Security Management). ISO 17799 includes encryption as a best practice in information systems security management.

[48] I conclude that the measures EFAP took to protect the personal information held in its custody were clearly inadequate and did not meet the standard of reasonable security measures required by s. 30 of FIPPA. This conclusion does not impose a standard of absolute liability (that is, a standard in which there is no defence of due diligence when loss occurs). Rather, applying the objective test of reasonableness found in s. 30, and the considerations mentioned in Investigation Report F06-01, it is clear that EFAP, and thus VCHA, did not meet the statutory standard.

What protective measures have now been put in place?

[49] Following the theft, EFAP retained a security guard while an alarm system was installed and the regular glass beside the entrance door was replaced with reinforced glass. Full physical security measures have since been installed at EFAP to protect the computer equipment. These include security cables on all ancillary equipment such as routers, modems and monitors.

[50] The server has been moved to a physically secure server room with a locked, entry-resistant door and a secure lockable server cabinet bolted to the concrete floor. More recently, a secure server was also installed to provide a high level of data security, with hardware and software firewalls, high-level user authentication and individual permission/access levels.

[51] EFAP is continuing to search for either an alternative application or a custom upgrade of its client database software to further improve security and is exploring encryption options. Password access for all users has been implemented with a minimum 8 character, case-sensitive combination of letters, numbers and symbols that must be changed every 90 days.

[52] EFAP has been informed by its commercial landlord that options are being examined for the installation of security cameras in the two remaining unmonitored exits, although installation is a challenge due to the heavy concrete structure.

[53] In the area of policies and procedures, a draft set of guidelines has now been prepared by VCHA to address best practices for protection of computer equipment and portable devices and EFAP's Confidentiality & Security Guidelines have been amended to include specific protection measures for office premises, computer equipment and data and software security enhancement. It is apparent that these policies will remain a work in progress, in order to

support appropriate evolving standards in the area of identity management and access controls.

[54] **3.7 Issues in the Notification Process**—FIPPA imposes on public bodies a duty to take reasonable security arrangements against various unauthorized activities, including those unauthorized activities related to access, collection, use, disclosure or disposal. On the face of s. 30, there is no duty to notify individuals affected by a potential unauthorized access, disclosure or use.

[55] In Investigation Report F06-01, the Commissioner indicated that, in appropriate cases, s. 30 may require a public body to notify affected individuals, as a reasonable security measure. He noted that a report[3] by Paul Chadwick, Privacy Commissioner of the Australian State of Victoria, and factors mentioned in a California statute requiring notification of individuals in certain cases, were both useful in assessing whether a public body should notify individuals affected by a loss of personal information. Commissioner Loukidelis then went on to say this:

> [106] …In my view, the key (but not sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed. The harm-assessment approach, I note, has also been used by the Office of the Information and Privacy Commissioner for Alberta in investigations into personal information security breaches under Alberta's *Personal Information Protection Act*.[4]

[56] A public body should, following a data loss or theft, conduct a prompt assessment of any risks posed thereby. If the public body concludes that notification is appropriate, viewed in light of s. 30 as discussed in Investigation Report F06-01, it should prepare a notification strategy and execute it.

[57] The public body should proceed on the basis that early notification is generally preferred to later notification, in order to give affected individuals the best opportunity to take whatever defensive measures are appropriate.

[58] In determining whether notification is appropriate, Commissioner Chadwick's report, quoted with approval by Commissioner Loukidelis, articulated a useful test in which the potential harm to data subjects resulting from the

[3] *Jenny's case: Report of an investigation into the Office of Police Integrity* (Report 06-01). http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/27DAEE1EBC21E085CA257123000A3688/$FILE/OVPC_Report_0106.pdf.

[4] The Commissioner was referring here to Alberta Investigation Reports P2005-IR-001 and P2005-IR-002, found at www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf and www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf.

breach is weighed against the potential harm resulting from the notification process itself. It is worth repeating the text of that test:

> In deciding whether the circumstances of any case are exceptional such as to make notification neither necessary nor desirable, the following factors should be considered in context by an appropriately senior decision maker in possession of the relevant facts –
>
> 1 The potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved (referred to as the 'data subjects') or others affected, having regard to:
>
> - the nature of the information, in particular its sensitivity;
> - the amount of information;
> - the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online;
> - any relationship between the recipient/s and the data subjects;
> - the degree to which the data subjects may already be aware of the breach of their information privacy and be able themselves to minimise harm;
> - the steps taken by the organisation to contain the breach and minimise harm.
>
> 2 The potential for notification itself to cause reasonably foreseeable harm to the data subjects (or any other person), excluding potential harm to those responsible for the breach (such as damage to reputation, or exposure to disciplinary action or claims for redress, or bad publicity).
>
> 3 Whether, considering 1 and 2, notification is reasonably likely to alleviate more harm than it would cause. [5]

[59] As this passage indicates, one issue to be considered, which EFAP did consider in its deliberations, is whether notification to individuals may itself cause harm. EFAP's main concern was to attempt to notify clients in a manner that did not reveal an individual's confidential relationship with EFAP. A related concern for EFAP was whether broadcast notification by email or by regular mail addressed to all employees would cause emotional or psychological harm to vulnerable clients.

[60] One of the underlying principles of privacy protection is that individuals have the opportunity to exercise a measure of control over their personal information. It is the client more than anyone else who will have an appreciation of the consequences of disclosure and of the steps necessary to prepare for or cope with the fact of disclosure. Notification was the only means by which a client could acquire a measure of control in these circumstances.

[5] *Jenny's Case*, ibid.

[61] It is not necessary in this case to decide whether the circumstances warranted notification as VCHA, following its own deliberations, concluded that it should notify affected individuals. I will therefore discuss the process of notification in this case. I will discuss both the method of notification and the timing.

The notification process in this case

[62] As noted above, EFAP notified VCHA executive staff about the March 25 theft on March 27 and 28. As VCHA had not had previous experience with this type of security breach, it convened an executive meeting on March 28 for the purpose of assessing options. The outcome of that meeting was a decision to contain the information about the breach within the management group until the clinical impact of the potential disclosure of personal information could be assessed. On March 31, representatives of VCHA's executive staff, legal counsel and senior management informed the OIPC of the circumstances to date by way of a conference call.

[63] The small group of EFAP employees whose financial information was at risk (Class 1) was given notice by telephone or in person at their place of employment on March 31. As part of a general risk mitigation effort, and due to risk of identity theft flowing from the presence of SINs and other personal data, the notification included an offer of a subscription to a credit monitoring service to provide timely warning of any unusual financial activity occurring under the employee's name.

[64] VCHA received a verbal briefing on the stolen data access security risks from its security consultant April 3rd, followed by a written report April 6. On April 5, VCHA obtained an opinion on the preferred options for notification from a registered psychologist. One option proposed in the opinion was notification by letter. The opinion cautioned that organizations should not engage in a broadcast notice to their employees, because the broadcast of the information would "cause greater harm than good". The consultant psychologist proposed that the employer should be copied with the wording of the letter written to employees.

[65] Union representatives for employees of public bodies and organizations that EFAP served were notified of the breach on April 6. At noon on April 6, the VCHA sent an internal email to all VCHA staff and to the administration of the other health authorities and private sector organizations served by EFAP, with a request that these other authorities similarly notify their staff. This notice advised employees who had utilized EFAP services to call a confidential helpline if they were concerned. This encompassed Classes 2 and 3, with the exception of clients who were no longer employees of these organizations. VCHA also undertook to contact the 1,300 individuals who were at special risk (Class 2) by telephone. VCHA declined initially to engage in a public notification program as

suggested by the OIPC on April 4, but did acknowledge that "the matter has rapidly become public regardless"[6] and therefore decided to do it.

[66] VCHA had difficulties with the telephone notification process, relating to the logistics of dealing with a large volume of calls, contact difficulties, and concerns about maintaining confidentiality of the purpose of the call with respect to calls answered by third parties. It abandoned the telephone notification approach after attempting calls to about 50% of the clients identified as having clinical notes on the stolen computer system. Successful personal contact was made with approximately 23% of the clients called, representing about 11% of the 1,300 clients with Class 2 information. As a substitute for telephone notification, EFAP chose to do a generic mail-out to all clients (information Classes 2 and 3) that had given EFAP permission to mail correspondence to their residence and for whom EFAP still had an address for mailing on file. VCHA and EFAP held the view that this type of non-personal broadcast mailing would enable the information to be sent out without creating an awkward situation (implied or potential breach of client confidentiality) for the recipient.

[67] For the broadest form of notification, including notice to former employees of organizations served by EFAP, VCHA drafted a newspaper advertisement that ran in a series of major and community newspapers between April 29, 2006 and May 5, 2006, depending on individual publication dates (see Appendices 1 and 2).

Analysis of notification outcomes

[68] This section assesses the notification process with reference to Classes 1, 2 and 3 and considers the adequacy of notification measures adopted by EFAP and the timing.

[69] <u>Class 1:</u> Employees of EFAP whose contact and payroll information (including SIN) was stored on the stolen computer. This group was notified by telephone March 31, six days after the theft.

[70] By virtue of the small number of affected individuals and the nature of the information (personal but not intimately so), this group could be notified easily without difficult issues arising pertaining to personal vulnerability. However, the nature of the information stored meant that the employee's financial interests could be jeopardized in a very short period of time, thus making prompt notification essential.

[71] EFAP's manager of administration noted that it took a few days for EFAP to thoroughly review all EFAP's back-up documentation in order to provide a complete inventory of the stolen data. The immediate focus of this inventory process was to accurately identify the extent and nature of the confidential client

[6] Email communication with VCH Executive April 7, 2006.

information at risk. As a result, the fact that personal employee information was also stored on the stolen computer did not come to light until several days after the theft. The manager also stated that it was not standard practice for EFAP to keep such data in electronic format past the initial employee sign-up; in this case, it had been done for the 10 most recent EFAP employees. Upon discovering this information, the affected employees were notified within 24 hours and were provided with the appropriate resources including, as noted previously, credit monitoring services.

[72] This fact highlights the importance for organizations of understanding what information is held in their computing facilities. A failure to keep pace with and be aware of the scope of personal information held by an organization increases vulnerability generally through a misapprehension of existing risk. It can also increase the period of delay prior to breach notification. If there is no backup database or other source of information to determine the scope of data affected by the breach, proper notification and adoption of defensive measures may never happen at all. In this case, the notification mechanism was reasonable and the risk mitigation strategy was appropriate, but the delay in identifying the individuals affected could have been reduced through compliance with appropriate data security and records management policies.

[73] Class 2: This is the group of approximately 1,300 individuals whose files were closed and whose clinical counselling notes were held in a separate data file in Adobe portable document format (.pdf). As noted in the previous section, EFAP attempted to notify these individuals by telephone, but stopped about halfway through the exercise, as it was becoming increasingly clear to EFAP that it was difficult to maintain client confidentiality in the context of telephone notification. As discussed earlier in this report, this is a vulnerable group by virtue of what one may expect to be intensely personal information contained in the counselling notes.

[74] It was the OIPC's view from the beginning that telephone notification presented at the client's workplace presented difficulties, even though the callers worked from a carefully prepared script. Calling individuals at their place of residence offered a greater probability of contact, but also a greater chance of inadvertent disclosure, or pressure to disclose, if a spouse or child answered the call and later asked the client about the reason for the call.

[75] The level of notification for Class 2 was adequate in the circumstances. Email notification (2 weeks post-breach) was followed by attempted telephone notification (2+ weeks post-breach), then by generic notification by regular mail, supplemented by newspaper advertising (4 to 5 weeks post-breach). I conclude the strategy that was ultimately implemented was reasonable but the delay, occasioned primarily as a result of VCHA's efforts to develop that strategy, was less than acceptable. Fear of adverse consequences for clients, while consistent with EFAP's mission to help and support, prevented EFAP from taking reasonable steps in a timely manner to get out an effective notification.

[76] Class 3: This class covers the more than 9,500 EFAP clients with personal information on file, including contact information and issues presented at initial counselling sessions. This constitutes the largest and potentially most diverse group in terms of interests and vulnerability. An internal email notice was sent out approximately two weeks post-breach. Broader notification by way of advertising in community newspapers had not yet taken place as at one month post-breach.

[77] Indirect publication by way of a notice to all employees over an organization's internal email network, or broadcast notification in the form of newspaper advertising, would be an acceptable form of notification if combined with a mechanism for supporting those clients who have concerns about the consequences of the data theft. Those support options could include FAQs posted to a website and a toll-free telephone number for contacting an information helpline staffed by knowledgeable persons who can provide guidance with respect to a range of options for protecting the client's interests.

[78] Consistent with OIPC's early suggestion, and at considerable effort, EFAP, in consultation with VCHA and the organizations to which EFAP provides services, set up a telephone helpline, with carefully researched information scripts, to answer questions from concerned clients. EFAP actually found a net positive response, in that a number of callers who were not clients previously were interested in and wanted to avail themselves of EFAP's counselling services. EFAP also discovered that the vast majority of individuals calling the helpline (over 90%) were fully satisfied by the explanation they received and did not wish to pursue the matter any further. A summary chart of EFAP's client responses as compiled by the helpline is attached to this report as Appendix 3. It is worth noting that the advertising initiative produced virtually no responses to the helpline; this may be a result of the fact that by the time the advertisements appeared, the issue of the breach had become public, and those clients who were concerned had already contacted EFAP.

[79] As with Class 2, it appears that a concern with doing the best thing for its clients delayed EFAP in taking decisive action to do the right thing for its clients. It was important and appropriate for EFAP to obtain expert guidance from consultants with a view to undertaking a proper notification program. This consulting effort with attendant internal discussions and meetings, however, took time, not least because it was being done for the first time.

[80] The result is that notification of current employees of health authorities and related organizations by way of broadcast email was adequate in form, but delayed. Notice to ex-employees by way of community advertising was likewise delayed—a period of over one month post-breach is not acceptable by any standard. If one takes the view that notification is necessary, then notification should be timely, notwithstanding that the scope of risks to which a data subject might be exposed cannot be determined with precision. Concern for the welfare

of clients resulted in notification delays that were, in my view, not consistent with the purpose of notification, which is to permit parties potentially affected by the breach to take appropriate action in response. What constitutes "appropriate action" will in large measure be a decision of the client after being informed of the risks and options for response.

4.0 DEVELOPING APPROPRIATE POLICIES AND PRACTICES

[81] As noted above, the standard for the protection of personal information is set out in s. 30 of FIPPA. In order to satisfy that standard, public bodies should develop reasonable and appropriate policies and practices. Public bodies should ensure that appropriate safeguards are in place so that personal information in their custody or under their control is secure; these safeguards will assist public bodies in preventing privacy breaches. Public bodies also need to develop policy for dealing with a privacy breach should a breach occur despite the safeguards.

Safeguards

[82] The circumstances of this case—involving both a small and a large organization—highlight the need for all public bodies (and organizations in the private sector) to plan for and take tangible steps to secure personal information in their custody or under their control. In protecting personal information, steps involved in meeting the reasonable security measures standard under s. 30 of FIPPA will include these:

- Understand what personal information you hold in your systems. Conduct a periodic inventory of the kind and sensitivity of personal information held in your databases and establish a policy by which staff responsible for data security are informed of any change to the scope of personal information held. Hold only what you need, according to the business-related purpose for which it was collected, and only for as long as you need it;

- Conduct a physical security audit or have a qualified professional do it. Understand the physical risk of hardware theft or other loss and the particular vulnerabilities of your office environment and take steps to protect against such threats. Develop a written policy concerning physical security and ensure that staff follow it;

- Implement defensive measures to guard against unauthorized data access, both external and internal, and whether resulting from a hardware theft, employee misconduct or system intrusion by hackers. In considering the possible range of measures to implement, public bodies may wish to seek guidance from ISO 17799 (Code of Practice for Information Security Management) or comparable generally-accepted information security standards. Of particular importance is the sensible option of encrypting personal information to make sensitive personal information extremely difficult to access by any unauthorized individual. Again, develop a written policy governing data security in your organization.

[83] Attached to this report as Appendix 4 is an example of a list of privacy safeguards that can be used to develop an organization specific set of safeguards. Appendix 4 includes a discussion of several issues beyond the factual context of this report that should nonetheless be addressed by public bodies and private sector organizations. In particular, Appendix 4 includes a reference to safeguards for portable computing devices such as laptop or notebook computers that are at greater risk of theft. For such devices, encryption may be the most effective measure to guard personal information held on the devices.

Breach Policy

[84] Neither EFAP nor VCHA had policies—often referred to as a "breach protocol"—in place to direct organizational response to a privacy breach. Even with a policy, not all circumstances can be predicted or planned for. The process of determining an appropriate response is time-consuming, but becomes disproportionately so without the benefit of a policy to guide the response efforts. In addition, judgements on delicate issues in such an environment are often made under stress, which may produce a sub-optimal outcome. For these reasons, a policy prepared in advance can be indispensable.

[85] A breach policy should include a plan for dealing with the consequences of data losses. What is the scope of the data loss? What measures are required to contain the breach? If personal information is stolen, how might it be used? Who will be affected? Should affected individuals be notified and if so, how? What will be the content of notification and what risk-management strategies should you deploy to assist your clients in mitigating the risks to which they have been exposed? What information will you need to answer client questions in the event of a breach?

[86] A guide to responding to privacy breaches—which is not the same as an organization-specific breach policy, but that can be used to create one—is attached to this report as Appendix 5.

5.0 CONCLUSION

[87] I conclude that VCHA, through its EFAP program, did not meet the requirements of s. 30 of FIPPA respecting protection of personal information. However, it is clear that, leaving aside the above-noted concerns about delay in

the notification process, VCHA—which co-operated fully with this investigation—has taken this security breach very seriously and continues to address the deficiencies I identified in my investigation.

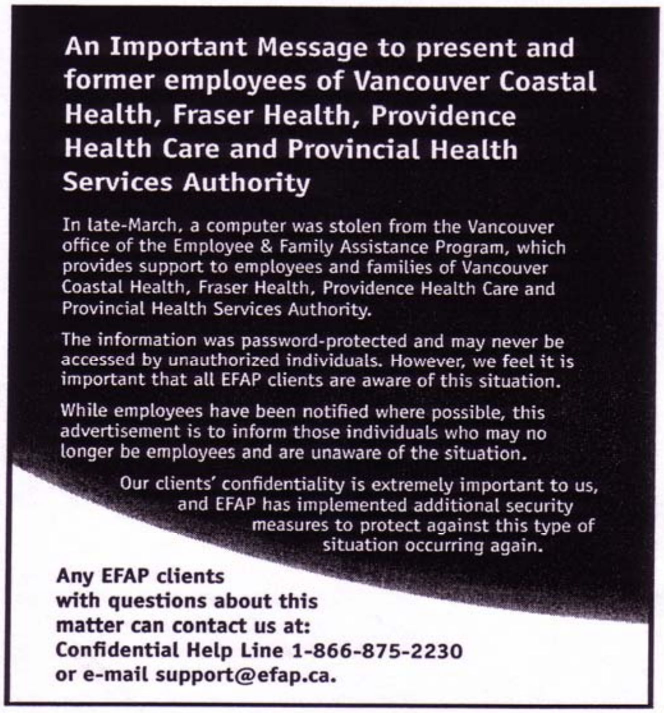
June 7, 2006

ORIGINAL SIGNED BY

Michael Skinner
Portfolio officer

OIPC File No. F06-28366

APPENDIX 1



An Important Message to present and former employees of Vancouver Coastal Health, Fraser Health, Providence Health Care and Provincial Health Services Authority

In late-March, a computer was stolen from the Vancouver office of the Employee & Family Assistance Program, which provides support to employees and families of Vancouver Coastal Health, Fraser Health, Providence Health Care and Provincial Health Services Authority.

The information was password-protected and may never be accessed by unauthorized individuals. However, we feel it is important that all EFAP clients are aware of this situation.

While employees have been notified where possible, this advertisement is to inform those individuals who may no longer be employees and are unaware of the situation.

Our clients' confidentiality is extremely important to us, and EFAP has implemented additional security measures to protect against this type of situation occurring again.

Any EFAP clients with questions about this matter can contact us at: Confidential Help Line 1-866-875-2230 or e-mail support@efap.ca.

APPENDIX 2

NEWSPAPERS

- Vancouver Sun
- The Province
- Victoria Times Colonist
- Nanaimo News Bulletin
- Kamloops This Week
- Kelowna Capital News
- Penticton Western
- Abbotsford News
- Aldergrove Star
- Burnaby News Leader
- Chilliwack Progress
- Hope Standard
- Langley Times
- Maple Ridge News
- Mission City Record
- New Westminster News Leader
- North Short Outlook
- Peace Arch News
- Richmond Review
- South Delta Leader
- Surrey Leader
- Tri-City News

APPENDIX 3

VANCOUVER COASTAL HEALTH AUTHORITY
EMPLOYEE & FAMILY ASSISTANCE PROGRAM
SECURITY BREACH RESPONSES – SUMMARY REPORT
• APRIL 6, 2006 TO MAY 26, 2006 •

I. SUPPORT LINE & EMAIL INQUIRIES:

QUERIES RECEIVED	#	%
Number of toll-free calls	85	67.5%
Number of emails	41	32.5%
Total # of Queries	**126**	**100%**

NATURE OF QUERIES	#	%
Questions re: Information & Security	91	72%
Questions about accessing EFAP	20	16%
Supportive calls	10	8%
Address Updates	5	4%

SUMMARY OF RESPONSES	#	%
Positive/Satisfactory Outcome	109	86.5%
Concerned & Directed to Risk Mgmt	3	2.4%
No Response Required	6	4.8%
Unable to Contact	8	6.3%

The data above reflects the queries received as a result of four different forms of notification, during two different time periods. The first form of notification was through broadcast email to active employees. Immediately subsequent to the employee email, there were media responses that provided more public notice of the breach via newspaper and radio. About 50% of the above queries are from these first two forms of notification that occurred in early to mid April.

The final two forms of notification commenced at the end of April and were by direct mail-out and published newspaper ads. A notice to "employees and former employees" prepared by VCH Communications was printed in 24 newspapers throughout BC (both provincial and community). The same notice was directly mailed to approximately 8000 EFAP clients, which represents almost 73% of our client base. These clients were selected based on the fact that they had given us permission to send them correspondence when they first accessed our program, and that we still had a complete address on file for them. To date, approximately 11% of the 8000 notices have been returned as undeliverable. Almost all of the queries received during this second notification period (50% of the above) were from the direct mail-outs.

In general, we have experienced that our clients have been mostly relieved to learn that our client data did not include any Social Insurance Numbers, banking information, employee ID or healthcare numbers. There were a few clients who had their phone numbers & addresses unlisted so expressed more concern than others about having this basic contact information on our system.

In most situations, we were able to look-up each client's status in advance and if we identified them as one of the inactive clients who also had clinical notes on the stolen system, we would inform them of this at the time of our response. The majority of the responses have been positive and supportive to our program.

II. TELEPHONE NOTIFICATION:

CALL BREAKDOWN	#	%
Number of wrong #s	171	26.5%
Number of clients reached	148	23%
Number of unavailable clients	326	50.5%
Total number of clients called	**645**	**100%**
3rd party contacts - % of all calls	35	5.4%
3rd party contacts - % only of clients reached		23.6%

RESPONSE BREAKDOWN	#	%
Clients report OK with call & info	144	97.3%
Clients unhappy with call & info	1	.7%
Clients referred to Risk Mgmt	3	2%

Along with the information we typically collect from our clients for our client database, we had also identified that there were approximately 1300 inactive clients who had scanned clinical notes on the stolen system as well. These scanned notes were in the process of being archived. It was acknowledged that these clients in particular should be informed that there was more detailed confidential information regarding their use of the EFAP then for most clients. It was decided that the EFAP should attempt to contact these clients directly by telephone where possible. This telephone notification started the same day as the first email notification was sent out, but the bulk of the calls were made on the Saturday and Sunday following. Senior level EFAP therapists worked in shifts of four, with some administrative support, at the EFAP's main office on both days.

As with the responses from the call-backs summarized on the first page, we experienced that our clients were relieved to learn that our client data did not include any Social Insurance Numbers, banking information, employee ID or healthcare numbers. There was some concern expressed about the fact that there were also scanned clinical notes from their case on the stolen computer, but this was lessened once we explained how these notes were identified and stored in relation to the client database. Again, primary concern was about the possibility of identity theft.

We found that initially we needed to spend significant time explaining who we were, why we were calling, and how we obtained their name and number. We often met with initial distrust around our identity and purpose of our call. We also found that reaching 3rd parties was very uncomfortable and in many cases we were concerned about compromising confidentiality and increasing risk. Our concern for further compromising the confidentiality of our clients and potentially increasing the level of risk in their household continued to increase with each new contact with a 3rd party. After we completed the scheduled Sunday shift, we stopped the unsolicited telephone notification process. We had called about half of the identified clients and had only reached about 11% of the total.

We were fully supportive of continuing with notification, however, based on our experience with the telephone process, we felt it necessary to explore other methods that may not compromise confidentiality at the same level as these unsolicited phone calls. After discussion with the relevant parties, it was determined that publishing a general notice to "employees and former employees" in local newspapers, and directly mailing this general notice to identified clients, would be the least compromising method to reach the targeted individuals (see summary results on page 1). Our initial concerns about protecting client safety by not publicly disclosing details of the theft were no longer as relevant since there had already been public notification through the various media responses.

APPENDIX 4

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

PHYSICIANS & SECURITY OF PERSONAL INFORMATION

May 2006

The Information and Privacy Commissioner for British Columbia is concerned about recent privacy breaches involving personal health information and the adequacy of security measures being used to protect patient records. This is a reminder that private sector organizations, including physicians in private practice, are required by BC's *Personal Information Protection Act* (PIPA) to take reasonable security measures to protect personal information from risks such as unauthorized collection, use or disclosure. PIPA sets out the consequences for violations of these requirements.

In a recent report on the sale of provincial government back-up computer tapes containing the sensitive personal information of British Columbians, the Commissioner said that meeting the reasonableness standard is not a matter of simply doing one's best to protect personal information. "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."[7] The Commissioner also indicated that costs should not be the determining factor when assessing the adequacy of security. The back-up tapes were sold at a public auction of provincial government assets and when the purchaser realized the tapes contained personal information they were turned over to *The Vancouver Sun*.

Where a privacy breach has occurred, please see "Key Steps in Responding to Privacy Breaches" for steps to take, including notifying the College of Physicians and Surgeons available at: http://www.oipc.bc.ca.

THEFT OF COMPUTERS & OTHER MEDIA

Criminal activity is a risk that must be considered when assessing whether security arrangements are reasonable.

[7] Sale of Provincial Government Computer Tapes Containing Personal Information, Investigation Report F06-01, p. 14, para 49, http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf.

SAFEGUARDS TO CONSIDER

- Appoint a member of your organization who will have overall responsibility for security. Your organization will already have a Privacy Officer so it may make sense to also give them responsibility for security. Develop a security plan and include the risk of theft of your computers in the plan. Make sure everyone in your organization is aware of his or her security responsibilities.

- Increase the number of barriers that will deter, if not stop, a thief from stealing records containing personal information. Barriers may include:

    - Enhanced exterior security, including alarms and lighting;
    - Minimizing interior vulnerabilities by controlling public access and reducing the visibility of computers;
    - Using physical security, such as bolting computers to the desk or storing paper records in locking cabinets.

- If possible, store patient and employee personal information on an on-site network server that is in a secure location.

- Data back-up plans should be developed, implemented and regularly audited.

- If electronic records containing sensitive personal information, such as a patient's diagnostic information, are being stored on desktop computers, laptops or a server, or your computers are connected to the internet, a reasonable security precaution would be to use both password protection and encryption to protect the information. Encryption is defined as a method to obscure information so that it is unreadable by anyone but those who are intended to read or receive the information.

- If a laptop containing sensitive personal information is taken off site, the data should be password protected and encrypted. The laptop should be in your control at all times. Consider locking laptops in a secure place after working on them at home.

- The use of a password to protect sensitive personal information will not, by itself, meet the test of reasonable security measures.

OTHER RESOURCES

RCMP IT Security Bulletin: Guide to Minimizing Computer Theft. This bulletin can be downloaded from the RCMP's Technical Security Branch website at: http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/index_e.htm

SECURITY OF ON-SITE PATIENT RECORDS

An organization must make a reasonable effort to ensure their paper records containing patient personal information are protected from theft, unauthorized access or unauthorized disclosure.

Safeguards to Consider

- Store records securely in locking cabinets or behind locked doors whenever possible.
- Clearly label records.
- Lock cabinets and doors when access to records is not necessary.
- Return files to the filing location as soon as possible after use.
- Store records in such a way that members of the public can not accidentally view the contents of files.
- If files need to be removed from the office, use a formal "booking out" system to track there whereabouts.
- If files are transferred to another office, track the transfer by confirming that the record arrived at its destination.

Other Resources

BCMA, *Guide to Ensuring the Security of Patient Records.* This document can be downloaded from: http://www.bcma.org/public/news_publications/publications/privacytoolkit/guidetoensuringsecurity.pdf

FAXING AND EMAILING PERSONAL INFORMATION

You should not fax or email sensitive personal information unless speed of transmission is essential. If faxing or emailing are the only timely methods available, extra precautions are required.

Safeguards to Consider

- Set rules about the types of personal information that can be faxed or emailed to or from your organization. Document your rules and check regularly to confirm employees are following the rules.

- Locate your fax machine in a secure area to control access and to prevent unauthorized persons from viewing faxed information. When faxing sensitive information, monitor the machine during the faxing process.

- Phone ahead to confirm the fax number and email address before sending personal information. Confirm the security arrangements for receiving faxes and emails. Ask the intended recipient to call as soon as possible to confirm receipt of the email or fax.

- Use encryption technology to email and fax sensitive personal information.

- Never use an email distribution list to send sensitive personal information.

OTHER RESOURCES

Office of the Information & Privacy Commissioner for British Columbia ("OIPC"), *Faxing & Emailing Personal Information*. This can be downloaded from: http://www.oipc.bc.ca/pdfs/public/fax-emailguidelines(Feb2005).pdf.

TRANSPORTING RECORDS BY COURIER

Choose a courier company that has implemented the security safeguards listed below. It is vital that they demonstrate that they consistently practice these safeguards.

SAFEGUARDS TO CONSIDER

- Ask the courier company what security measures it employs to protect personal information. Some measures that should be employed are:
    - Physical security in their offices and areas where the personal information is stored, including locked storage, alarms and monitoring;
    - Restricting employee access to personal information;
    - Ensuring drivers are bonded and insured;
    - Having staff sign confidentiality agreements;
    - Driver guidelines and policy that ensure the personal information is kept secure while in the vehicle; and
    - A method to track the shipment of records that requires the receiver's signature.
- Ensure the courier company tracks the shipment and collects the signature of the receiver when the delivery is made.
- The sender should record an itemized description of the documents being transported in case there is a discrepancy about what documents were received, or in case any missing files need to be identified.
- When transporting records containing personal information by courier, consider calling the receiver to confirm pick up and ask them to confirm receipt of the records.

DESTRUCTION OF RECORDS

Physicians should establish clear policies regarding the destruction of medical records containing sensitive personal information. Procedures should be taken so that confidentiality is maintained when documents are destroyed.

Safeguards to Consider

- *Physical Records*

  Physical destruction of records should be done in a way that prevents the information on the records from being retrieved or reconstructed. Shredding is the generally accepted way to destroy paper records containing personal information.

  - When considering the destruction of medical records, physicians should be aware of the College of Physicians and Surgeons of British Columbia's retention guidelines, the provisions of the *Limitations Act* and any requirements of their insurers.

    - The most secure methods of destroying paper records, in order of effectiveness, are: in-house cross shredding; in-house ribbon shredding; a shredding service that comes to your office to shred; and shipping intact records off site for shredding.

    - If you are considering an off-site shredding service, it is important to ensure that you choose a shredding service that is experienced in destroying sensitive records and that it has policy and procedures in place to ensure confidentiality during the destruction process. Ask the shredding service what security measures it employs to protect the records. Some measures that should be employed are:

      - Physical security in their offices and areas where records are stored, including locked storage, alarms and monitoring;
      - Restricting employee access to records;
      - Ensuring drivers are bonded and insured;
      - Having staff sign confidentiality agreements;
      - A method to track the shipment of records and their destruction; and
      - Providing customers with a certificate of destruction.

- *Electronic Records*

  - Computerized medical records must have the same sensitivity and confidentiality considerations applied. Simply deleting computer files, or reformatting a disk does not securely destroy the data. It is generally believed that when a deleted file is overwritten with new data, the old data is destroyed. According to data recovery experts, this is not true and data can be recovered from overwritten disks.

  - The secure way to destroy data is by "wiping". Wiping is the process of writing and re-writing blank data over the disk until all traces of the original data are destroyed. Specialized software is required to securely wipe a disk.

- You should also consider the physical destruction of securely wiped hard drives, CD/DVDs, tapes, USB disks and other storage media as a method of completely destroying data.

OTHER RESOURCES

The RCMP published a March 2006 IT Security Bulletin that reviewed then available disk-wiping software products. The bulletin can be downloaded from the RCMP's Technical Security Branch website at: http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/index_e.htm.

The College of Physicians and Surgeons of British Columbia's *Medical Records in Private Physicians' Offices* is part of the College's on-line Resource Manual for Physicians and can be downloaded from: https://www.cpsbc.ca/cps/physician_resources/publications/resource_manual.

BCMA Privacy Toolkit:
http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/ToolKitTableOfContents.html

Ontario Information and Privacy Commissioner: *Fact Sheet on Secure Destruction of Personal Information.*
http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=16713&N_ID=1&PT_ID=15825&U_ID=0

This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. Its contents do not fetter, bind, or constitute a decision or finding by, the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization and public body.

APPENDIX 5

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

KEY STEPS FOR PHYSICIANS IN RESPONDING TO PRIVACY BREACHES

May 2006

The most common privacy breach happens when personal information of your patients or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed or faxed to the wrong person.

You must respond at once to a privacy breach. You should take Steps 1, 2 and 3 below immediately after a privacy breach in order to mitigate the effects of a privacy breach.

Rapid action after a privacy breach is part of your responsibility for protecting personal information. British Columbia law requires private and public sector organizations to take reasonable security measures to protect personal information against unauthorized disclosure or use.

This is a summary guide to responding to privacy breaches.

Step 1 Contain the Breach

- Immediately contact your privacy officer or the person responsible for security in your organization
- Notify the police if the breach involves theft or other criminal activity
- Immediately contain the breach by seeking return of the records, shutting down the system that was breached, correcting weaknesses in physical security, etc.

Step 2 Evaluate the Risks Associated with the Breach

To determine what further steps are immediately necessary, first assess the risks associated with the breach considering the following factors:

- What kinds of personal information are involved? (The more sensitive the information, the greater the risks.)

- What is the cause of the breach? Is there a risk of ongoing or further exposure? Was it stolen, lost or mistakenly disclosed (if the last, to which kind of organization?)
- Approximately how many individuals are affected by the breach? Are they inside or outside your organization?
- Is the information encrypted or otherwise not easily exploited?
- Can the information be used for fraudulent or otherwise harmful purposes?
- What kind and extent of harm to individuals might result from the breach (including risk to public health, identity theft, loss of business or employment opportunities, hurt, humiliation, damage to reputation or relationships)
- What harm might your organization suffer due to the breach (e.g., loss of trust, loss of business, loss of assets or other financial exposure)

Step 3 Notification

The key consideration is whether you should notify affected individuals of the breach to avoid or mitigate harm to them. You should review the risk assessment under Step 2 to assess whether notification is required and to address the following notification considerations.

Who you should notify

There are four groups of individuals that may require notification:

- Individuals whose personal information is involved in the breach.
- Other organizations that may be affected by the breach.
- Other groups may require notice based on legal, professional or contractual obligations. In the case of self-governing professions, contact the regulatory body. The regulatory body may receive calls from the public concerning the breach.
- The Office of the Information and Privacy Commissioner for British Columbia (OIPC)[8].

How to notify individuals affected by the breach

You can notify affected individuals directly or by a substitute method. Choose the method that will most effectively mitigate the harm you have identified. Also consider whether the direct approach could be too privacy-invasive in the particular case. Substitute notification can include sending a general notice to groups that include affected individuals or publication of a notice through the media.

[8] The following factors are relevant in deciding when to report a breach to the OIPC: the sensitivity of the personal information, whether the disclosed information could be used to commit identity theft, whether there is a reasonable chance of harm from the disclosure including non pecuniary losses, the number of people affected by the breach and whether the information was fully recovered without further disclosure.

What to include in the notification

Notifications should include the following pieces of information:

- The fact that a privacy breach occurred and a description of it
- The elements of personal information involved
- The steps you have taken to mitigate the harm and any likely further steps
- Advice to affected individuals on what they can do to further mitigate the risk of harm
- The fact that affected individuals have a right to complain to the OIPC or the BC College of Physicians and Surgeons.

Step 4 Preventing Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach (including through a security audit of both physical and technical security). This should drive development of adequate long-term safeguards to prevent further breaches. You should review and update your policies to reflect the lessons learned and should refresh staff training on privacy obligations under British Columbia's applicable privacy law.

* * *