BRITISH COLUMBIA MEDICAL ASSOCIATION

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

COLLEGE OF PHYSICIANS & SURGEONS INCORPORATED 1886 VIRTUTE ET VERITATE BRITISH COLUMBIA

PHYSICIANS & SECURITY OF PERSONAL INFORMATION

June 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."[1] 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.

[1] 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/Investigation ReportF06-01.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