ALBERTA
INFORMATION AND PRIVACY COMMISSIONER

Report on the Investigation into Health Information Discovered on Hard Drive

Associate Medical Clinic
Airdrie, Alberta

June 23, 2003

Investigation Report # H0252

I. Introduction

[1] On May 28, 2003, a television broadcaster reported the discovery of health information on the hard drive of a used computer purchased by an individual in Calgary, Alberta. The records/information contained health information related to medical care and treatment provided by physicians at the Associate Medical Clinic (the Clinic).

[2] The Commissioner ordered an investigation into this matter under section 84(a) of the *Health Information Act* (HIA). This report outlines the findings and recommendations of this Office.

II. Background

[3] The physicians at the Clinic provide health services as defined in section 1(1)(m) of the HIA.

[4] In April of 1998, the Clinic retained the services of a transcriptionist. The transcriptionist worked from her home on her personal computer transcribing physician's medical notes and typing referral letters.

[5] In approximately February of 2002, the transcriptionist's computer stopped working and she began to pursue a warranty replacement. The transcriptionist advised me that her computer had locked up and she was unable to access and delete files. She returned the computer to the store where it was purchased. She said that she conveyed her concern that the hard drive contained confidential information to an employee at the store's customer service counter where she had initially purchased the computer. She claims that the customer service staff told her that computers with a hard drive problem are returned to the manufacturer where the hard drive is destroyed. Accordingly, she decided to return the computer and was provided with a new one. The hard drive was not destroyed. The store says that it is not their practice to destroy hard drives on returned computers.

[6] The faulty computer was sold to a salvage company. The computer re-entered the market place, where it eventually ended up at a store that buys and sells used goods, where it was subsequently purchased. In May of 2003, the purchaser saved health information onto a floppy disk and anonymously sent the information/records to a television broadcaster saying that they had purchased the computer from the used goods store. The floppy disk contained the health information of approximately 200 patients of the Clinic. The information/records are some of the information/records that were previously transcribed by the transcriptionist.

[7] I have examined the records/information saved onto the floppy disk provided to the television broadcaster. The disk contains diagnostic, treatment and care, health services provider and registration information. The records/information is 'health information' as defined in section 1(1)(k) of the HIA.

[8] Alberta's HIA came into force on April 25, 2001. This law applies to custodians, which includes physicians and other health service providers paid by the Alberta Health Care Insurance Plan to provide health services. The physicians at the Clinic are custodians. The law also applies to an affiliate of a custodian. The HIA defines an affiliate as an individual employed by a custodian, a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian. Therefore, the transcriptionist is an affiliate of the physicians at the Clinic. Custodians must ensure that their affiliates comply with the HIA.

III. Steps Taken by the Custodian

[9] The Clinic examined the records/information on the floppy disk to identify the patients affected. The Clinic tried to track the location of the computer so steps could be taken to confirm that they had retrieved all health information, and to ensure that the health information on the computer's hard drive had been properly destroyed. Unfortunately, the computer has not yet been tracked. The individual who had purchased the computer did not identify him or herself, and information that could identify the computer was not maintained when it was sold and re-sold on more than one occasion.

[10] The Clinic wrote a letter to each affected patient to advise them of the privacy breach.

IV. Assessment

[11] Section 60 of the HIA requires custodians to take reasonable steps to maintain safeguards to protect health information. This includes safeguards related to protecting the confidentiality of health information, the privacy of individuals who are subject to that information, any reasonably anticipated threat to the security and integrity of health information or loss of health information, and unauthorized access, use, disclosure or modification of health information. The safeguards must include appropriate measures for the proper disposal of health information.

[12] Section 63(1) of the HIA requires custodians to establish or adopt policies and procedures to implement the HIA.

[13] In this situation, the Clinic had an agreement with the transcriptionist concerning the work to be performed and the rate of pay. The Clinic also required the transcriptionist to sign an oath of confidentiality.

[14] The Clinic advised me that they have policies and procedures in place, however they pre-date the HIA. The Clinic says that they are in the process of updating these policies and procedures to comply with the HIA.

[15] Regulation 8(3) of the HIA requires that a custodian periodically assess its safeguards in respect of confidentiality, privacy and security of health information. While the Clinic was in the process of reviewing its policies and procedures, an assessment of safeguards had not yet been completed since the HIA came into force.

[16] This is an unfortunate situation that involves custodians who take the confidentiality and privacy of their patients seriously. In this situation, I do not believe that the custodians foresaw the risk of unauthorized access to this health information. However, the HIA requires that an assessment of safeguards take place to try and anticipate possible risks and ensure that reasonable safeguards are in place to mitigate the risk. Despite the best intentions of custodians and their affiliates, they may not be aware of how to properly dispose of a computer that contains sensitive health information. As such, I make the following recommendations:

V. Recommendations

1. Complete an assessment of the administrative, technical and physical safeguards presently in place to protect health information. One such safeguard should be:

    - Disposition of computer data storage components (i.e. hard drives, etc.) or portable media (i.e. tapes, diskettes, etc.) containing health information that require exchange or disposal should be destroyed (i.e. physically crushed, etc.), or the health information should be permanently deleted through use of a commercial disk wiping utility.

2. Ensure that affiliates are aware of and adhere to these safeguards.

3. Complete review of all policies and procedures and update them to comply with the HIA.

4. Ensure that agreements with affiliates, especially those who handle health information off-site, state that affiliates must comply with the HIA and the custodian's policies and procedures. The agreement should include specific direction related to the secure storage and disposal of health information during the course of the agreement, and at termination of the agreement.

[17] I request that the Clinic provide the Commissioner with a written report outlining the status of their work on each of the above recommendations within 90 days of the release of this report.

Submitted by,

LeRoy Brower
Health Team Leader