



**Michael Whitt**

# Health Service Provider Fined \$10,000

Michael Whitt and LeRoy Brower

Michael Whitt is a partner with Borden Ladner Gervais in Calgary; LeRoy Brower is the Director, Health Information Act, Office of the Information and Privacy Commissioner in Edmonton, Alberta



**LeRoy Brower**

In a precedent setting case, a medical office clerk from Calgary plead guilty to a charge of improperly accessing another person's medical information, in contravention of the Health Information Act (HIA). The individual appeared in court April 13, 2007 and was fined \$10,000. This is the first time charges have been laid and successfully prosecuted under the HIA.

The medical office clerk was found to have accessed the health information of the wife (the victim) of a man she was having an affair with. The clerk and the victim's husband who were "high school sweethearts" began an intimate affair shortly after the victim was diagnosed with ovarian cancer. The clerk was employed by a plastic surgeon in a medical clinic in Calgary and had been given access to Alberta Netcare, which is the provincial electronic health record system. The clerk, without authorization, accessed the victim's lab test, biopsy and CAT scan results through Alberta Netcare, and by fax, 17 times on six different occasions for personal reasons.

When the affair ended, the victim's husband told her the medical clerk had accessed her health information. The victim subsequently filed a complaint with the Information and Privacy Commissioner of Alberta.

The health information in Alberta Netcare can be accessed by authorized users for the purpose of providing a health service. The plastic surgeon was not providing a health service to the victim or involved in her treatment or care. Alberta NetCARE's security features include strong auditing capability. A footprint is left for every access that shows the login ID of the accessing individual, the specific information that was accessed and at what time. The Commissioner's investigation found evidence confirming the accesses

of health information that occurred, which included Alberta Netcare audit logs.

Results of the Commissioner's investigation were presented to Alberta Justice's Regulatory Crown Prosecutor's Office and the Information containing the charges was sworn on November 6, 2006.

The clerk was charged under HIA section 107(2) (b). This section says:

*107 (2) No person shall knowingly  
(a) gain or attempt to gain access to health  
information in contravention of this Act,*

Alberta's Information and Privacy Commissioner Frank Work said this case should serve as a clear message to all health care custodians and their employees. "This is a very serious matter, and health care providers must know that surfing records for personal purposes will not be tolerated and individuals will be prosecuted. My office is charged with protecting the health information of Albertans, and we will not hesitate to recommend charges again in the future."

Information relating to the provision of health services to individuals in Alberta is protected by the Alberta HIA. "Health information" (or the local equivalent) in other Provinces is protected by similar special-purpose health information legislation, or mechanisms found in privacy legislation (egs. FOIP, PIPA or PIPEDA) and health sector legislation (egs. Hospital Acts and Medical Professions Acts). The protections are not all as specific as the Alberta HIA section noted above.

The Alberta HIA (and similarly, other health-specific information protection regimes) provides authority for health service providers to access and share personal health information for specific purposes (such as to provide care, to audit medical service payments, to provide prescription drugs, etc), but only for those legitimate purposes. The legislation has enabled the institution of large-scale data networks and information repositories (electronic health records), and permits

sharing of personal health information from a number of sources as needed to provide high quality care based on current and complete information.

Electronic health records enable access to health information by many (thousands) authorized health service providers. This arguably supports the well informed and efficient delivery of health care services, but it comes with a risk - the risk of unauthorized access.

To mitigate risk, health service providers have, in addition to duties under the HIA, subscribed to a variety of policies, information manager agreements, license and service agreements, and other arrangements that bind them to properly access, use, disclose and protect personal health information. This provides education, guidance, governance, and sanctions to promote and protect the trust necessary for both patients and providers alike to rely upon and candidly use modern information systems in healthcare.

In addition to the legislation, the following are important mechanisms to help protect and instill that important level of trust and mitigate the risk of unauthorized access:

- Policies and procedures (including prohibitions against surfing personal health information records)
- Privacy and security training
- Confidentiality oaths
- **Strong auditing capability** (competent systems will have robust logging functions that leave a footprint of who, what and when information was accessed)
- Periodic review of policies and procedures to ensure they have been effectively implemented
- Periodic review of safeguards to ensure they continue to mitigate risk, meet legal requirements and industry best practices

- **Active audits** (periodic review of system logs for unusual or unauthorized activity such as looking at a celebrity record or patient with the same last name etc. – this should include advising employees of auditing capability and that active audits are done to deter browsing)

Right to ask the Commissioner to conduct a review  
Governments and healthcare providers have identified the need to take protection of personal health information very seriously, and to safeguard and build the trust in healthcare information systems required for their proper and full utilization.

The Alberta Commissioner's office has merely been the first involved in the prosecution of data surfing, or gaining access for unauthorized purposes of health information in an electronic health record. It can safely be assumed that Privacy Commissioners (or Ombudsmen) in every jurisdiction in Canada will investigate similar complaints and take a strong stance on improper access of health information for personal reasons.

The best advice we can give to practitioners in health informatics areas? **Do everything you can reasonably**

## New Edition! Guidelines for the Protection of Health Information

**Essential** for minimizing risk, maximizing integrity and protecting privacy for all personal health information.

**Relevant** content aligned with Canada Health Infoway requirements and national and international standards such as the CSA model privacy code and ISO 17799.

**Practical** tenets of privacy legislation & principles outlined in clear language related to health-specific content.

**Customizable** for diverse jurisdiction-specific privacy policies.

2006 edition now available ONLY from  
COACH as Downloadable PDF

Order online at [www.coachorg.com](http://www.coachorg.com).  
Jurisdictional rates available.

For more information, contact the  
COACH office at (416) 494-9324  
or toll free at 1-888-253-8554.  
E-mail: [info@coachorg.com](mailto:info@coachorg.com).

