IPC
PERSPECTIVES
INFORMATION AND PRIVACY COMMISSIONER / ONTARIO

VOLUME 15
ISSUE 1
SPRING 2005

ANN CAVOUKIAN, Ph.D., COMMISSIONER

Commissioner Ann Cavoukian (second from right) with her new executive: Assistant Commissioners Ken Anderson (left) and Brian Beamish, and Janet Geisberger, Director of Corporate Services. **See story on page 3.**

Toronto Police Services Board scraps fee, tells police chief to work with IPC

One of the more compelling challenges facing police services across Ontario today is the need to balance the retention of personal information for investigative purposes against individual privacy rights.

Recently, the Toronto Police Services Board proposed a revision to its policy on the retention of photographs and fingerprints of individuals who have been charged – but not convicted – of criminal offences.

Currently, police policy dictates that all individuals who have been charged, but not convicted, of a criminal offence have a right to have their fingerprints and photographs destroyed by submitting an application to the police. There is no cost associated with this application. Under the proposed policy revisions, Toronto police would have a discretionary authority to refuse applications for destruction of such personal information for charges related to "serious" crimes (i.e., crimes involving guns, violence or sex offences). In addition, a $50 fee would be imposed for all applications for record destruction.

When the proposed policy revisions were initially unveiled last summer, Information and Privacy Commissioner Ann Cavoukian wrote a letter to the Toronto Police Services Board outlining her concerns.

The Commissioner emphasized that the proposed changes would be "contrary to commonly accepted principles underlying the presumption of innocence that exist in our criminal justice system" and that any

CONTINUED ON PAGE 8

In this issue:

Toronto Police Services Board scraps fee

Recent IPC publications

Upcoming presentations

New senior team at the IPC

When health information custodians work for non-health custodians

Profile: Robert Binstock

Order summaries

Mediation success stories

Recent IPC Publications

The IPC has issued (in order of publication) the following publications since the last edition of *IPC Perspectives*:

Your Health Information: Your Rights. The IPC and the Ministry of Health jointly produced this eight-panel brochure. October 2004.

Privacy Review: Video Surveillance Program in Peterborough. This review was launched in response to a complaint about the program. December 6, 2004.

Collection, Use, Disclosure and Other Complaints. This brochure explains that, if you feel that a health information custodian has inappropriately collected, used or disclosed your personal health information, or does not have proper information practices in place, you have a right to make a complaint to the IPC. December 2004.

Access and Correction Complaints – Personal Health Information Protection Act. This brochure explains what to do if an individual is not satisfied with the outcome of his or her request for access to or correction of personal health information, and how to file a complaint with the IPC. December 2004.

I'm Sorry, this Meeting is Closed to the Public: Why We Need Comprehensive Open Meetings Legislation in Canada. Assistant Commissioner Tom Mitchinson presented this paper at the annual conference of the Council on Governmental Ethics Laws (COGEL) in San Francisco on December 6, 2004.

Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Shared Services Bureau, Management Board Secretariat, and the Ministry of Finance. December 16, 2004.

Your health information: Your access and correction rights, is a fact sheet outlining some of your rights under the *Personal Health Information Protection Act*. January 2005.

Safeguarding Personal Health Information, is another *PHIPA* fact sheet. January 2005.

Ontario Regional Poison Information Centres and the 'Circle of Care,' is a *PHIPA* fact sheet. March 2005.

All of these publications and more are available on the IPC's website at www.ipc.on.ca.

Upcoming Presentations

June 2. Commissioner Ann Cavoukian is delivering a keynote address at the Canadian InfoSec Summit 2005 in Ottawa.

June 2. Ken Anderson, Assistant Commissioner (Privacy), is a guest speaker at the annual ethics conference sponsored by the St. Mary's Hospital ethics committee, at the Kitchener/Waterloo Sunshine Centre, Kitchener. His topic is: *Managing Health Information: PHIPA and the Role of the IPC.*

June 3. Commissioner Cavoukian is delivering the keynote address at the Fourth Workshop on *The Economics of Information Security*, at the Harvard Privacy Lecture series, Harvard University, Cambridge, MA. The title of her presentation is *The Economics of Privacy: Go Beyond Compliance to Competitive Advantage*.

June 10. Commissioner Cavoukian is speaking to the P.E.I. Association of Medical Radiation Technologies at the 63rd annual *CAMRT Conference* in Charlottetown. Her topic is *Privacy and Health Information*.

June 16 & 17. Assistant Commissioner Anderson will be leading a breakout session, *Taking the Temperature of Ontario's Health Privacy,* and participating in a Commissioners' panel at *Access & Privacy Conference 2005* in Edmonton.

Commissioner's new senior team at the IPC

By Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/
Ontario

I want to bring everyone up to date on some significant changes at the senior staff level at the IPC. Among these, I have appointed two new Assistant Commissioners, one after the retirement of long-time Assistant Commissioner, Tom Mitchinson.

Among the changes are:

- The appointment of IPC veteran Ken Anderson as the Assistant Commissioner for Privacy;
- The appointment of Brian Beamish, who has been with the IPC for six years, as the Assistant Commissioner for Access; and
- The retirement, at the end of 2004, of Assistant Commissioner Tom Mitchinson, who had been with the IPC virtually since our doors first opened.

Ken Anderson, who has held senior positions with the IPC for 15 years, was the Director of Legal and Corporate Services when appointed as Assistant Commissioner for Privacy. Ken, who has also been designated as the Assistant Commissioner under the new *Personal Health Information Protection Act,* has played a vital role in ensuring the IPC is prepared to meet its responsibilities as the oversight agency under that *Act,* which came into effect Nov. 1, 2004. Under our new, streamlined structure, the director or manager of our Corporate Services, Legal and Policy departments all report to him.

Ken, who taught privacy law at the University of Ottawa for three years, earlier led the IPC's administrative tribunal division both as Director of Appeals and as Assistant Commissioner for Access. Ken began his career in litigation, quickly developing a practice in the areas of administrative law and public sector administration. He received his law degree from the University of Western Ontario, and a degree in business administration from the Ivey School at the University of Western.

Brian Beamish, who joined the IPC in 1999 as Director of Policy and Compliance, was serving as Director of Policy, Compliance and Communications – directing IPC research, policy development and communications efforts – when I appointed him as the Assistant Commissioner for Access. In his new role, Brian directs the Tribunal Services Department. The Registrar's Department, Adjudication Department and Mediation Department all report to him.

Before joining the IPC, Brian held various senior positions with the Ontario ministries of the Solicitor General, and Correctional Services. A graduate of the University of Toronto Law School, he was called to the Ontario Bar in 1982.

Brian has demonstrated his leadership qualities time and time again. He has led numerous public- and private-sector projects for the IPC, addressing issues such as the interplay between privacy and technology and a number of cross-jurisdictional initiatives, including one with the U.S. Department of Justice.

Though I have two excellent new Assistant Commissioners, we have also lost a very valuable member of the team. **Tom Mitchinson,** who retired in December as Assistant Commissioner for Access, was a key executive for the IPC since the early days of this office. A leading expert on freedom of information legislation, he helped launch our popular schools' program (including teachers' kits on access and privacy) and directed a major restructuring of the Tribunal Services Department. All of us here wish Tom all the best in his retirement.

Another recent change among senior staff was the appointment of **Janet Geisberger**, who joined the IPC in 2000 as Manager of Corporate Services, as the first Director of Corporate Services, a key position in our new structure. Janet has also been appointed to the four-person IPC executive. The Communications, IT and Administration departments all report to her.

Janet, who has an extensive background in human resources, has a Bachelor's Degree in Economics from Wilfrid Laurier University, and

CONTINUED ON PAGE 8

When health information custodians work for non-health custodians

When the *Personal Health Information Protection Act* (*PHIPA*) came into effect November 1, 2004, the term *health information custodian* was unleashed on an unsuspecting public.

PHIPA, the first Ontario privacy *Act* to cover any part of the private sector, covers the broad health sector. As more than health care practitioners are covered under the legislation (for example, nursing homes and long-term care facilities, community care access corporations and boards of health are also covered), another term was needed.

Health information custodians are individuals or organizations listed (because of profession or role or specific duties) in the legislation because the individual or organization has custody or control of personal health information.

The largest group of health information custodians is comprised of *health care practitioners*. The term health care practitioner is defined to mean a person who is a member of a regulated health profession, and who provides health care.

Essentially, *PHIPA* applies to institutional and individual health care providers who have custody or control over personal health information. This includes almost anyone who provides health care, such as physicians, nurses, hospitals, long-term care facilities, pharmacists and social workers. It also applies to certain other entities that have different roles in the health care system, such as the Ministry of Health.

In order to ensure compliance with *PHIPA*, it is imperative for health care providers to determine whether they are considered a health care practitioner that provides health care within the scope of *PHIPA*. In many situations, health professionals will find themselves employed as agents of a health information custodian, as in the case of a nurse who works for a hospital. In this circumstance, the hospital (organization), not the nurse (practitioner), would be considered the custodian that bears the ultimate responsibility for meeting the requirements of *PHIPA*.

In some instances, health care practitioners may find themselves employed, or acting on behalf of, entities whose primary purpose is not the provision of health care. For example, a nurse may be employed by a school or a factory, a physician may work for a professional sports team or an insurance company, or a registered massage therapist may provide services to clients at a spa. Health care practitioners who work or volunteer in such settings are considered to be health information custodians and subject to the rules of *PHIPA*, if they provide health care. In addition, if a custodian delegates responsibilities to a non-health information custodian employee, that custodian himself or itself is responsible for the non-custodian's compliance with *PHIPA*.

When it comes to health information custodians working for non-health information custodians, one of biggest causes of concern has been, and still is, an employer having access to the personal health information of its employees.

Some health information custodians may find themselves in a position where they have been asked by their employer to disclose the personal health information of a particular employee. Such requests are often for legitimate purposes – for example, accommodating a safe return to work after an injury or to determine eligibility for sick or disability leave. Here, it is important to remember that, unless authorized by law, a warrant, a collective bargaining agreement, or in other limited circumstances, a custodian must obtain the express consent of the individual when disclosing personal health information to an employer. For employers, it is important to remember that *PHIPA* limits any collection, use or disclosure of personal health information to the minimum required to meet the identified purpose of the request.

Moreover, *PHIPA* also regulates non-health information custodians that are recipients of personal health information from health information custodians. This is informally referred

Continued on Page 9

A year of change for IPC registrar

When a privacy complaint or an appeal against a decision by a government organization denying a freedom of information request is filed with the IPC, it comes to Robert Binstock's *intake* team.

Binstock, the IPC's *registrar,* has the authority to screen out privacy complaints or appeals that do not fall within the *Acts* that the IPC has oversight responsibility for, and to stream appeals and privacy complaints that do qualify to other stages in the process. He is also responsible for directing the administrative support staff of the Tribunal Services Department.

"Each file is different and presents a unique set of circumstances and challenges for myself and the intake staff," said Binstock.

IPC Registrar Robert Binstock

But after years dealing with appeals and complaints under two *Acts* – the *Freedom of Information and Protection of Privacy Act*, which came into effect Jan. 1, 1988, and the *Municipal Freedom of Information and Protection of Privacy Act*, which came into effect January 1, 1991 – the IPC became the oversight agency for a third *Act* when the *Personal Health Information Protection Act* (*PHIPA*) came into effect Nov. 1, 2004.

Binstock spent much of last summer preparing for the implementation of *PHIPA*.

(In brief, under *PHIPA*, an individual may complain to the IPC if he or she feels his or her personal health information has been collected, used or disclosed in a way contrary to the legislation. Individuals also have the right to access or correct their personal health information. If such an access or correction request is denied, an individual can file a complaint with the IPC.)

"We spent a great deal of time determining how these complaints should be processed through the intake, mediation and review stages," said Binstock. "We also recruited additional staff that could bring their experience in the health care sector to the Tribunal Services Department. We relied on our past experience to develop policies and procedures for processing health privacy complaints. This was a challenging and exciting time."

Looking forward, Binstock will spend part of this year making adjustments to the complaint processes for *PHIPA*. "Now that we have had several months of experience, we will be able to fine-tune the process."

Binstock, who graduated in 1980 from York University with a Bachelor of Arts Degree in geography and urban studies, joined the Ontario public service in 1982, as a human rights officer for the Ontario Human Rights Commission. During his tenure there, he also completed a one-year secondment as a search officer for the adoption disclosure register of the Ministry of Community and Social Services.

He joined the IPC in 1989 as an appeals officer, and later held the positions of inquiry review officer and appeals supervisor. He was appointed registrar in 1999, when the structure of the Tribunal Services Department was reorganized.

Binstock's interest in technology has allowed him to identify and implement methods for improving the efficiency of IPC processes and make things easier for the public to understand. For example, he designed and implemented an automated flow chart for various stages of the public sector appeals and complaint processes, and adapted it for the new *PHIPA* legislation, providing users of the IPC website site (www.ipc.on.ca) with a ready source of information on various IPC processes, all organized from the same design framework.

Binstock and his wife, Martha, have two sons, Aaron, 16, and Jason, 19 (currently on a three-month educational excursion to Europe). Aaron plays competitive volleyball, so many of the family's weekends are spent at tournaments across North America.

Summaries

"Summaries" is a regular column highlighting significant orders and privacy investigations.

Order MO-1865-I
Appeal MA-030326-1
City of Toronto

During the spring and summer of 2003, the City of Toronto (the city) experienced a serious health crisis when severe acute respiratory syndrome (SARS) was detected in a number of area residents. The city later received a request under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) for access to all records created at the beginning of the outbreak. The requester specified that he did not want any information that would identify SARS patients.

The city granted **partial access** to a total of 197 pages of responsive records, relying in part on section 14(1)(f) (unjustified invasion of privacy) of the *Act* to deny access. During the appeal, the requester – now the appellant – took the position that additional records should exist and the adequacy of the city's search was added as an issue. The city subsequently identified 38 additional pages and claimed that section 14(1)(f) applied to all of them. These new records were included in the scope of the appeal.

Section 14 of the *Act* only applies when the information at issue qualifies as "personal information" as defined by the *Act*. In this appeal, the IPC adjudicator's determination of whether the information qualified as personal information turned on the question of whether there was a reasonable expectation that an individual could be identified were the information disclosed.

Disclosure of some information, including names, addresses, telephone numbers, birthdates and family status, would clearly identify individuals or SARS patients. References to identification numbers assigned to the SARS patients and patients' relationships with other individuals contacted by public health officials could also identify patients. As the requester had asked that all "identifying information" be removed, the adjudicator ordered the city to sever all such information.

The adjudicator found that once the personal information of the various patients – including their names and the relationships between the patients and other individuals – was removed, there was no reasonable basis for concluding that tracking histories related to SARS patients would identify any specific individuals. He ordered disclosure of this information.

However, the adjudicator found that disclosure of information relating to clinical tests, symptoms or treatment of specific SARS patients coupled with information about early SARS patients from other public sources could identify the patients and should be withheld. He made an exception for information relating to SARS generally or patients not otherwise directly identified in the record. He found there was insufficient evidence to establish a nexus between the information and the patients that would identify a specific individual, and ordered this disclosed.

The adjudicator also ordered that information detailing the activities of officials managing the early days of the crisis be disclosed, as they neither made references to individual SARS patients, nor could they lead to the identification of any patients. The adjudicator found that the names and other related information, such as business addresses and phone numbers of physicians and health officials who had contact with SARS patients, did not qualify as "personal information" as it related to their professional responsibilities. However, where health care professionals themselves became SARS patients, the adjudicator found that this type of information qualified as the physicians' "personal information," and this information was withheld.

Assessing the adequacy of the search conducted by the city, the adjudicator found that there were some gaps in the record-gathering process that had not been adequately explained. He ordered additional searches as well as an affidavit from the city's medical officer of health identifying all officials in the city's public health department who might have responsive records in their files and attesting to the various search activities performed.

Order PO-2367
Appeals: PA-040047-1
Ministry of Health and long-Term Care

The Ministry of Health and Long Term Care (the ministry) received a request under the *Freedom of Information and Protection of Privacy Act (the Act)* for all records relating to the ministry's request for proposal (RFP) process for CT and/or MRI services at *independent health facilities* to be located in

CONTINUED ON PAGE 9

Mediation Success Stories

"Mediation success stories" is a regular column highlighting several of the recent appeals that have been resolved through mediation.

Having the right parties at the table led to resolution

The Ministry of Transportation (the ministry) received a four-part request under the *Freedom of Information and Protection of Privacy Act* (the *Act*) for records relating to an impending expropriation of property near a specified highway. After paying the fee set out by the ministry, the requester received access to most of the records that she had requested. The ministry withheld the remaining records on the basis that they contained personal information or valuable government information.

The requester, now the appellant, appealed the ministry's decision to the IPC on the basis that more records responsive to her request exist.

In her letter of appeal, she explained that the ministry had served her with expropriation papers for a part of her property for the purpose of highway expansion. This part has a cold-water stream, which runs into a wetland abutting her property.

During mediation, the appellant clarified that she is looking for a full environmental assessment report of her property, including the cold-water stream. The appellant noted that the ministry had disclosed a 2002 environmental study report to her but this record did not contain any reference to her property or to the cold-water stream.

The mediator conveyed this information to the ministry, which advised that it had provided the appellant with all responsive records. However, the ministry's special advisor for FOI suggested that it might be helpful to have the ministry employees who conducted a search for the records speak directly with the appellant.

A teleconference was arranged. The ministry's special advisor for FOI, the head of records, the project engineer for Hwy. 26 and the environmental planner for the planning and design department participated in the teleconference, along with the appellant, her environmental advisor and the mediator.

The ministry's staff explained to the appellant that a full environmental assessment is not the type of document produced by the ministry and it does not have such a record. More importantly, they also provided an explanation of the ministry's environmental assessment process and preliminary design through which the ministry considers the general impact on the environment and why there was no reference to the creek in the 2002 environmental study report provided earlier to the appellant.

The appellant indicated she understood the explanations provided by the ministry and advised that she was satisfied that the ministry does not have the record she is seeking. As a result of the ministry's efforts to explain why it did not have the record at issue, the appeal was successfully mediated.

Two computers stolen from hospital

A hospital advised that two computers went missing from the physiotherapy department. The hospital was faced with how to fulfil its obligations under the *Personal Health Information Protection Act* (the *Act*), including notification of affected patients.

The hospital's network was password protected, however, the hard drives of the two computers that were stolen were not. To determine what information was stored on the computers, staff were asked to describe what they recalled saving on the hard drives.

It was determined that the computers contained some patient "progress notes." These notes included patients' full names and described the reason these patients were seeking services, the services provided and the outcome. The computers also contained a list consisting of full patient names and respective "wards."

The hospital undertook verbal notification of each patient whose name or progress note was believed to have been stored on the missing computers.

This verbal notification was carried out using a document that the hospital created with the

Continued on Page 10

Toronto Police Services Board scraps fee

CONTINUED FROM PAGE 1

retention of photos and fingerprints of those not convicted of a crime should be severely limited. In response to the Commissioner's letter, the board decided to postpone a decision on the proposed new policy.

The issue subsequently came back before the board at its January 24, 2005 meeting, when Commissioner Cavoukian made a presentation to the board.

The Commissioner stressed that retention of photos and fingerprints of anyone arrested but not convicted (and with no previous convictions) should take place only in accordance with fair information practices establishing:

- that all non-conviction dispositions be treated in the same way;
- that any discretionary power to deny applications for destruction of fingerprints and photos be based on a clear set of criteria;
- that individuals be provided with notice that their fingerprints and photographs were being retained; and
- that no fee be charged for requests for destruction of fingerprints and photos.

Toronto lawyers Clayton Ruby and Avvy Go also made presentations opposing the proposed changes.

The board voted against the creation of the $50 fee for applications and passed a motion mandating that the chief of police consult with the Commissioner in order to develop specific criteria regarding any instances where photographs and fingerprints of those charged, but not convicted, may be retained.

From presentations and discussions at that police services board meeting, it became clear that there is no uniform policy across Ontario relating to the treatment of these records. Commissioner Cavoukian expressed a willingness to work with the Ontario Association of Chiefs of Police to formulate an Ontario-wide policy on this issue.

The Commissioner was pleased with the board's decisions. "I look forward," she said, "to working with Toronto's police chief, the Ontario Association of Chiefs of Police, and others in law enforcement on this issue."

New Senior Team at IPC

CONTINUED FROM PAGE 3

has completed the advance program in human resources at the University of Toronto and an executive program at the Richard Ivey School of Business. Janet worked for the Ministry of Transportation and the Ministry of Health before joining the IPC.

Among other appointments:

- **Mona Wong**, who joined the IPC in 1999, has been appointed Manager of Mediation. Mediation is our preferred method of resolving access appeals and privacy complaints at the IPC and Mona oversees the mediation process. She was the Team Leader of the IPC's municipal mediation team before her appointment as Manager of Mediation and has been a very key member of our Tribunal Services team. Before joining the IPC, Mona was the Freedom of Information Co-ordinator at the Ministry of Health.
- **Michelle Chibba** joined the IPC in April as our new Manager of Policy and Compliance and we are very glad to have her. Michelle has an extensive background in policy development. She was the Manager of Planning, Financial and Corporate Support for the Academic Health Sciences Centre, Alternative Funding Program, at the Ministry of Health and Long Term Care, prior to joining the IPC.
- Another very welcome addition is **Peter Khandor,** who joined the IPC in February as my Executive Assistant. Prior to joining the IPC, Peter articled and worked as an associate at the law firm Torys LLP. Peter received his law degree from Osgoode Hall Law School and was called to the Ontario bar in 2003. He also holds a Masters in Social Work from the University of Toronto.

I want to take this opportunity to thank my entire staff for their ongoing professionalism, dedication and hard work. I am very proud of my team and am grateful to have the opportunity to work with such professionals in support of open government and the protection of privacy.

Summaries

CONTINUED FROM PAGE 6

eight Ontario communities. During the processing of the request by the ministry, the requester narrowed the request to apply to only two specified providers (the affected parties).

The ministry located 12 records containing 1,808 pages as responsive to the request and denied access to them. The requester appealed the ministry's decision. During mediation of the appeal, the requester (now the appellant) narrowed the scope of the request to include only specified portions of the five successful RFP submissions by the affected parties. The appellant focused his request on specific identified information in the affected parties' RFPs.

The primary issue in this order is whether the ministry was entitled to apply the section 17(1) exemption (third party information) in the *Act* and deny disclosure.

The adjudicator examined whether the ministry satisfied each part of the three-part test under section 17(1). The adjudicator first determined that the information remaining at issue in the records qualified as "commercial information" within the meaning of section 17(1), satisfying the first part of the test. Next, he ruled that the records were clearly "supplied" to the ministry by the affected parties and that an article in the ministry's RFP, which indicated that the proposals would remain confidential, satisfied the "in confidence" requirement of part two of the three-part test.

As to the part three "harms" portions of the test, the ministry submitted that the disclosure of detailed operational, technical and trade secrets information relating to how the affected parties would operate their facilities would reveal details of their business operations and thereby cause harm to their competitive position. The ministry also suggested that should future RFPs be issued for these services elsewhere in Ontario, the affected parties would be at a disadvantage if their methodologies were revealed. The affected parties submitted that success in this industry requires the maintaining of a pool of trained employees and suggested a scenario of a "poaching" of their employees should the information be released.

The adjudicator found the affected parties and the ministry failed to provide the kind of "detailed and convincing" evidence required to uphold the ministry's decision not to disclose the records under part three of the three-part test. In the order, he stated that: "The affected parties have not provided me with specific references to the contents of the records in order to assist me in making a finding that disclosure of this information could reasonably result in any of the harms contemplated by section 17(1)."

Accordingly, the adjudicator ordered the disclosure to the appellant of the information about the RFPs sought by the appellant, except personal information such as home addresses, e-mail address and marital status.

Health information custodians working for non-health information custodians

CONTINUED FROM PAGE 4

to as the "recipient rule." For example, this means that a human resources officer, or supervisor/manager, who receives personal health information from a health information custodian who provides on-site health care, can only use or disclose that information for the purpose for which the health information custodian was authorized to disclose it, or to carry out a statutory or legal duty. The "recipient rule" only applies where personal health information is received directly from a health information custodian providing health care. *PHIPA* does not apply to personal health information disclosed by an individual employee to the employer.

Currently, organizations that collect, use, or disclose personal information during the course of commercial activities must comply with the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). This means that, in some cases, an employer of a health information custodian will be subject to *PIPEDA*. In the near future, the federal government is expected to deem the provisions of *PHIPA* to be substantially similar to *PIPEDA*. This ruling will likely exempt health information custodians that are covered under *PHIPA* from also having to comply with the provisions of *PIPEDA*.

If you, or your organization, have any questions regarding health information custodians, *PHIPA*, or *PIPEDA*, please contact us at info@ipc.on.ca, or visit our website, www.ipc.on.ca.

CONTINUED
FROM PAGE 7

assistance of the IPC. The document included a description of what had happened and described the steps taken by the hospital to contain the situation. Patients were told the police were contacted and that the computers were not recovered. Patients were also advised that the hospital was working with the IPC to ensure the hospital was meeting all the requirements under the *Act*. Contact information for the IPC was also provided.

The hospital implemented several measures to reduce the risk of a similar situation occurring in the future. Staff within the department, and all staff at the facility dealing with patient information on computers, were advised not to save personal health information on local hard drives. Department managers were asked to check computers to ensure patient information was removed from local hard drives and the hospital requested its computer support personnel to put a system or program in place that would result in documents from certain applications being saved as a default to the network. The facility also took steps to ensure new staff will receive guidance about the importance of not saving patient information to local hard drives.

The hospital also undertook some changes relating to the physical security, including changing the locks where the loss occurred.

Consent paved way to resolution of appeal

The Ottawa Police Service (the police) received a request under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) for a specific police report. The report was the result of an investigation into the requester's complaint that her telephone line was being monitored. She was also concerned about a call she had received from an unidentified individual at a number that she had subsequently traced.

The police granted partial access to the record and applied the law enforcement and personal information exemptions to deny access to the remainder.

The requester, now the appellant, appealed the decision to the IPC.

During the course of mediation, the police disclosed one page of the record in its entirety to the appellant.

As well as the appellant's information, the record contained the personal information of two affected persons: the appellant's husband and the individual at the traced number, whom the police had interviewed during the course of their investigation.

After being contacted during mediation, the appellant's husband and the other affected person consented to the disclosure of their information found in the record. This resulted in the disclosure of all of the information remaining at issue. Accordingly, the appeal was resolved.

IPC
PERSPECTIVES
is published by the **Office of the Information and Privacy Commissioner/Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée «Perspectives», est également disponible en français.

30% recycled paper

ISSN 1188-2999