

## RESOURCE CENTRE

### PRIVACY AND ACCESS TO INFORMATION



#### The Weakest Link: A Privacy Case Study and Cautionary Tale October 2, 2006

##### October 2006 Privacy and Access to Information

The single greatest privacy challenge facing institutions today does not lie in creating policies and procedures that are compliant with Canadian law. It lies in ensuring that those policies and procedures are followed and in taking swift, appropriate action if and when a breach occurs. This was made patently clear in the July 2006 decision of the Information and Privacy Commissioner of Ontario under the *Personal Health Information Protection Act, 2004*.<sup>[1]</sup>

Although based on Ontario legislation governing privacy of personal health information, the decision should be required reading for all private sector institutions in Canada that collect, use or disclose personal information. The questions to ask are: "If these facts arose in respect of our institution, what would we have done? Would the result have been any different?" Answers of "no", or "possibly not" are a call for immediate action by your organization.

#### HOW THE ISSUE AROSE

A patient was admitted to a hospital where her estranged husband and his girlfriend (a nurse) worked. The patient and her estranged husband were involved in a divorce and custody dispute. The patient took steps both before and at admission to highlight her concern that she did not wish her husband to know that she was in the hospital. She requested that her estranged husband and the nurse be prohibited from having any information regarding her hospitalization. Neither the patient's estranged husband nor the nurse were involved in the patient's care. The hospital took steps to ensure that the patient's estranged husband did not work in the area where the patient was. However, contrary to the hospital's privacy policy, the hospital's Chief Privacy Officer was not notified of the patient's concerns, and the matter was treated as a physical security issue only.

#### PATIENT LAUNCHES A COMPLAINT UNDER THE ACT

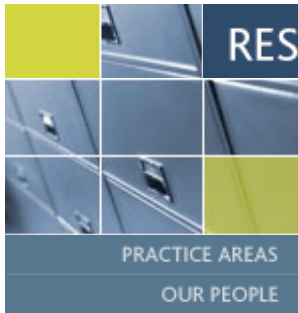
After her discharge from the hospital, the patient received a call from her estranged husband. It was apparent from that call that he was aware not only of her admission but also of her treatment. The patient made a complaint to the hospital under the Act and the hospital immediately commenced an investigation.

When the complaint was made, a protective flag was placed on the patient's file. The flag sent an audit report to the hospital's Chief Privacy Officer each time the complainant's record was viewed. The hospital's investigation revealed that the patient's file had been accessed by the nurse on seven occasions before the protective flag was added to the electronic record and on three additional occasions thereafter. The hospital's investigation also found that the estranged husband could only have learned the information about the patient from the nurse and concluded that a breach of the Act had occurred. The nurse was suspended for four weeks without pay; the estranged husband for ten days. The hospital also entered into confidentiality agreements with the estranged husband and the nurse confirming that they did not alter, destroy, copy or print any of the complainant's personal health information.

#### PRIVACY COMMISSIONER CONCLUDES REVISED PRACTICES ARE NECESSARY

The patient subsequently filed a complaint with the Information and Privacy Commissioner of Ontario. The findings made by the Commission included the following:

- the access by the nurse to the patient's electronic file was a use of personal health information in contravention of the Act by an "agent" of the hospital;
- the disclosure of the patient's personal information by the nurse to the patient's estranged husband was in contravention of the Act;



- the hospital did not take reasonable steps to protect the patient's personal information;
- staff of the hospital failed to follow internal policies; and
- the hospital failed to take immediate action to prevent further unauthorized access to personal information once notified of a possible breach of privacy.

In the course of her findings, the Commissioner stated that the hospital's human resources protocol for investigations resulted in a time delay of more than three weeks during which time the nurse continued to access the patient's file. The Commissioner found that delay to be unacceptable and ordered the hospital to review and revise its practices and procedures relating to patient health information and human resources to ensure that they comply with the requirements of the Act.

The Commissioner stressed that a "culture of privacy" must be created in healthcare institutions with policies "inter-woven into the fabric of a hospital's day-to-day operations". Employee education is critical. Above all, "predicating access on a 'need to know' basis could perhaps be no more important than in a healthcare setting, where so much is at stake".

In her findings, the Commissioner noted the "stellar efforts of the hospital's Chief Privacy Officer". Unfortunately, those efforts did not prevent the further instances of deliberate and unauthorized access to the patient's records.

## LESSONS LEARNED

The Commissioner's decision highlights the critical need to ensure that privacy policies and practices are complete, known and followed. Action items arising from this decision include the following:

- Employee education and clear policies governing when and how personal information may be accessed must be in place and followed. While it will be very difficult to guard against deliberate contraventions of privacy policies by employees, privacy policies and procedures for those who could come into contact with personal information should include a clear statement that any personal information may **only** be accessed on a "need to know" basis. Disciplinary measures and procedures should be reviewed to ensure that an institution is able to act quickly to contain a breach in the event of an occurrence.
- Institutions will not be able to avoid a finding of a breach of the Act by an employee if they have not taken thorough steps to prevent the breach.
- A thorough breach response plan is required and must cover all aspects of a response to a suspected breach, including containment measures, internal investigation, employee discipline, public relations response, and notification of affected individuals and the appropriate privacy commissioner. Complaints received by an institution concerning privacy should be dealt with immediately and responded to thoroughly.
- Security measures should be reviewed to ensure that they are adequate and must be assessed against a possible need (particularly in the healthcare context) to access personal records swiftly in the event of an emergency.
- Privacy initiatives must be openly supported by senior management.

Notwithstanding all these steps, no institution will be able to guarantee that there will never be a breach of the Act. However, by remaining vigilant, an institution may be able to minimize the effect of the breach on the individual concerned and the institution.

---

[1]. Information and Privacy Commissioner of Ontario, Order HO-002, July 27, 2006; available on-line at <http://www.ipc.on.ca/docs/ho-002.pdf>.

The purpose of this document is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of Ogilvy Renault LLP or any member of the firm on the points of law discussed.

For further information, please contact one of the following lawyers:

Penny S. Bonner	(416) 216-6629	<a href="mailto:pbonner@ogilvyrenault.com">pbonner@ogilvyrenault.com</a>
Christine A. Carron	(514) 847-4404	<a href="mailto:ccarron@ogilvyrenault.com">ccarron@ogilvyrenault.com</a>
Anne K. Gallop	(416) 216-4038	<a href="mailto:agallop@ogilvyrenault.com">agallop@ogilvyrenault.com</a>
Martha A. Healey	(613) 780-8638	<a href="mailto:mhealey@ogilvyrenault.com">mhealey@ogilvyrenault.com</a>
Dan G. Palayew	(613) 780-8637	<a href="mailto:dpalayew@ogilvyrenault.com">dpalayew@ogilvyrenault.com</a>
Russel W. Zinn	(613) 780-8672	<a href="mailto:rzinn@ogilvyrenault.com">rzinn@ogilvyrenault.com</a>

