Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

Executive Summary

Order HO-002

The Office of the Information and Privacy Commissioner/Ontario (IPC) received a complaint under the *Personal Health Information Protection Act, 2004* (the *Act*) involving the Ottawa Hospital (the hospital) in Ottawa, Ontario. The complainant claimed that during and after her treatment at the hospital as an in-patient, her personal health information was illegally accessed on ten known occasions, and some of that information was disclosed without her consent, to her estranged husband with whom she is in the midst of divorce proceedings, for an illegal purpose.

The IPC investigation found that the complainant, on entering the hospital for treatment, had informed the staff, that she did not wish her estranged husband, an employee of the hospital, or his girlfriend, a nurse at the hospital, to be aware of her admittance. She also did not want either individual to access her personal health information. Subsequently, following her discharge from the hospital, it became clear to her as a result of conversations with her estranged husband, that he was aware of her admittance to the hospital and details of her treatment. She then filed a complaint with the hospital.

Upon receiving the complaint, the hospital took immediate steps to flag the complainant's electonic health record (EHR) and audit all access to her EHR. The audit confirmed the complainant's position that the nurse had inappropriately accessed her EHR. However, the hospital did not immediately take steps to prevent the nurse from gaining further unauthorized access to her health information. The IPC investigation concluded that the nurse inappropriately accessed the complainant's EHR on three further occasions after the patient had complained to the hospital.

The IPC concluded that the nurse, as an agent of the hospital, used the complainant's personal health information and disclosed that information to the estranged husband, in contravention of the *Act*. Staff of the hospital failed to follow internal policies that specifically related to the protection of patients' privacy, and in so doing, failed to ensure the fullest protection of the complainant's personal health information. The hospital also failed to take immediate action to prevent any further unauthorized use of the complainant's personal health information, once notified by the complainant of the possible breach of her privacy.

Based on its investigation and these conclusions, the Commissioner ordered the hospital to take the following steps:

- To review and revise its practices, procedures and protocols relating to patient health information and privacy, and those relating to human resources, to ensure that they comply with the requirements of the *Act*, taking into account the paramount importance of protecting patients' personal health information;

- As part of this review to implement a protocol to ensure that reasonable and immediate steps are taken, upon being notified of an actual or potential breach of an individual's privacy, to ensure that no further unauthorized use or disclosure of records of personal health information is permitted;

- To ensure that all employees and/or agents of the hospital are appropriately informed of their duties under the *Act* and their obligation to comply with the hospital's revised information management practices.

The following Postscript by the Commissioner appeared at the conclusion of her order.

POSTSCRIPT

This was a truly regrettable situation in which a patient who was admitted to a hospital, made a specific request to prohibit her estranged husband and his girlfriend, a nurse at the hospital, from having any information regarding her hospitalization, only to learn that the exact opposite had occurred.

Despite having alerted the hospital to the possibility of harm, the harm nonetheless occurred. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach of this nature from occurring. In addition, the fact that the nurse chose to disregard not only the hospital's policies but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient's electronic health record, disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient's privacy by an employee of a hospital must be built into the policies and practices of a health institution.

This speaks broadly to the culture of privacy that must be created in healthcare institutions across the province. Unless policies are inter-woven into the fabric of a hospital's day-to-day operations, they will not work. Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital,

but must also ensure that privacy becomes embedded into their institutional culture. As one of the largest academic health sciences centres in Canada, the Ottawa Hospital had properly developed a number of policies and procedures; but yet, they were insufficient to prevent members of its staff from deliberately undermining them.

Health information custodians are responsible for ensuring compliance with the *Act* and are responsible for the actions of their employees and agents. I am taking this opportunity to remind all custodians of the importance of ensuring that their employees and agents are made fully aware and properly trained with respect to their obligations under the *Act*, as well as the need to create environments in which privacy issues are not only understood, but form an integral part of the culture of their institution. Despite the stellar efforts of this hospital's Chief Privacy Officer, the hospital's failure to follow through on its privacy policies at the time of the complainant's admission, followed by priority being given to a Human Resources Protocol over preventing further instances of unauthorized access to the patient's records, contributed in large part to the breaches reported. The ultimate responsibility, of course, lies in the actions of the two offending parties.

I strongly encourage all health information custodians, especially larger institutions such as hospitals, to take the need to protect patient privacy to heart. Upholding compliance with the Act is not simply a matter of following the provisions of an enacted law, but ensuring that the use and disclosure of sensitive personal information such as health information is strongly monitored, and access controlled to those who truly need it in the performance of their duties. 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. The negative consequences flowing from the unauthorized access and use of a patient's health information are extensive and far-ranging. Patients have enough to deal with – any additional stress arising from an unauthorized party peering into their health records is completely unacceptable.