



# An Invasion of Privacy

Protection of personal health information should be ingrained in a hospital's institutional culture

BY LONNY J. ROSEN

In October 2005, the Information and Privacy Commissioner of Ontario received a phone call from a newspaper reporter regarding documents containing personal health information that were strewn across a downtown Toronto intersection. Not knowing that the documents were patient health records, a film company was using the papers—which it had obtained indirectly through a paper recycling company—as a prop for a film shoot.

During a review of the case, the Privacy Commissioner determined that the health records came from a Toronto health clinic. The clinic had stored the health records in a designated storage area on the premises—much to the displeasure of the building's landlord, who eventually removed the boxes containing the health records and relocated them to the building's public parking lot.

## Wrongful disposal

Later, an employee of the health clinic found the boxes and transported them to another health clinic operated by the same management team. There, the documents were designated for disposal, but because they were too large to place in the shredding bin, they were placed in a back room. When a driver from a paper-disposal firm arrived to retrieve the documents, he assumed they were meant to be recycled (since they hadn't been shredded) and took them to a recycling warehouse. Eventually, a special-effects company contacted the paper-recycling firm to ask for scrap paper for use in a film shoot, and a box full of

these patient health records was sent to the film production company.

The case is a perfect example of how patient privacy can be violated when hospital staff doesn't understand provincial privacy laws, and when these laws are not interwoven into the fabric of a hospital's day-to-day operations.

Health professionals have always been legally required to maintain the confidentiality of their patients' personal health information. But the implementation of the *Personal Health Information Protection Act, 2004 (PHIPA)* in November 2004—arguably, the most significant development in Canadian health privacy law in recent years—advanced priva-

cy laws in Ontario. *PHIPA* provides uniform rules about how personal health information may be collected, used and disclosed by health professionals. Under the *Act*, health professionals are obligated to protect personal health information in their custody, and control it against theft, loss and unauthorized use or disclosure. They are also obligated to ensure that health records are retained, transferred and disposed of in a secure manner.

The Information and Privacy Commissioner of Ontario is the independent oversight body responsible for ensuring that health professionals collect, use and disclose personal health information in accordance with *PHIPA*. In 2005 and 2006, respectively, the Privacy Commissioner issued the first two orders under the *Act*. The first order set out its expectations of how health information custodians should dispose personal health information. The second order provided guidance on what steps are considered reasonable in the event of unauthorized access to, or disclosure of, personal health information in a hospital.

The unfortunate chain of events in the case involving the Toronto clinic led to its being found in violation of

privacy laws. The case serves as a reminder of the key principles of the Privacy Commissioner's first order. It stated that:

- Health information custodians are responsible for implementing a written agreement with any agent they retain to dispose of personal health information records. The agreement must set out the obligations for secure disposal and require the agent to provide written confirmation once he or she disposes of the health records;
- Secure disposal must consist of permanently destroying paper records by irreversible shredding, such as cross-cutting or pulverization, thus making them unreadable; and
- Health information custodians are responsible for ensuring that no unauthorized person will have access to the records throughout the disposal process.

### Silent invasion

In another case involving a separate hospital, a female patient was admitted to the emergency department and then transferred to the hospital's heart centre. Her estranged husband was an employee of the hospital, as was his girlfriend, who was employed as a registered nurse. On admission, the patient stated that she was concerned about the possibility that her estranged husband and his girlfriend would learn of her medical condition and hospitalization, and use this information against her in an ongoing custody battle. The hospital's medical staff recorded the patient's apprehension and noted that the estranged husband was not to be permitted to see her. The husband's manager was also notified to ensure that, during the patient's hospital stay, he did not work in the area where she was admitted.

Despite having taken these steps, the nurse, who was in no way involved in the patient's care, had accessed the patient's electronic health record on numerous occasions over a six-week period. The patient learned of this breach when

she received a call from her estranged husband who raised the issue of her heart condition and other information, which he could only have obtained from her hospital record. The patient then lodged a complaint about the unauthorized access to, and disclosure of, her health records.

In response, the hospital's chief privacy officer (CPO) placed a VIP flag on the patient's electronic health record, which did three things: notify any person attempting to access the record that the record had been deemed highly sensitive and that any attempt to view it would be closely monitored for potential invasion of patient privacy; prompt the user to choose whether he or she still wished to view the record; and automatically send an audit report to the CPO in the event the record was

ing the complainant's concerns," and by no means was it "a complete response," said the Commissioner. The Commissioner ordered the hospital to:

- review and revise its privacy and human resources policies to ensure that they comply with the requirements of the *Act* and its regulations;
- implement a protocol to ensure that reasonable and immediate steps are taken, upon being notified of an actual or potential breach of privacy, to ensure that no further unauthorized use or disclosure of records is permitted; and
- ensure that all employees and/or agents of the hospital are appropriately informed of their duties under the *Act* and obligations to comply with the revised informa-

**“ The Commissioner's message, which healthcare administrators should take to heart, is this: unless policies are interwoven into the fabric of a hospital's day-to-day operations, they won't work. ”**

viewed. The CPO also ordered an audit on the electronic health record, which confirmed that the nurse had accessed the file without good reason. The hospital took disciplinary action against the employees in question, suspending the nurse without pay for four weeks and the husband for 10 days. The hospital also required both of them to sign confidentiality agreements.

In this case, the Privacy Commissioner found the hospital did not take adequate steps to protect the patient's personal health information. The hospital's policies in these circumstances, the Commissioner found, were also insufficient to protect the patient's personal health information from further unauthorized access after the initial breach. Notifying the estranged husband's manager to ensure he avoided the area where the patient was staying was just a "starting point for address-

tion practices of the hospital. The Commissioner did not order—but strongly urged—the hospital to issue a formal apology to the complainant, as well.

The Commissioner's decision speaks broadly to the culture of privacy that must be created in healthcare institutions everywhere. The Commissioner's message, which healthcare administrators should take to heart, is this: unless policies are interwoven into the fabric of a hospital's day-to-day operations, they won't work. Hospital administrators must ensure they not only educate staff about the *Act* and privacy policies and practices, but also ensure that privacy becomes a value that is embedded into a hospital's institutional culture. **CHM**

.....  
*Lonny J. Rosen is a partner in the Health Law Group at Gardiner Roberts LLP.*