CANADIAN PRIVACY LAW REVIEW

Volume 12 • Number 9 August 2015

In This Issue:

Regulatory Colleges Respond to Health Privacy Breaches

Debbie Tarshis
Partner
WeirFoulds LLP

Sarah Yun
Associate
WeirFoulds LLP

Breaches of Health Privacy: Role of Professional Regulatory Colleges

The transition from paper-based patient records to electronic patient records appears to be resulting in an increase in privacy breaches by health professionals found "snooping" into patients' health records. Professional self-regulatory bodies have already had to grapple with this issue. The Discipline Committee of the College of Nurses of Ontario recently imposed a serious penalty on a member found guilty of such privacy violations, sending a message that such behaviour is unacceptable.

The legislation enacted to protect patients from unauthorized access to their personal health information, the *Personal Health Information Protection Act* [*PHIPA*],[1] has recently celebrated its ten-year anniversary. There has been only one prosecution under *PHIPA* since its inception, and it was dismissed last year by the court for delay. The Information and Privacy Commissioner of Ontario ("IPC") and the Ontario Minister of Health and Long-Term Care ("Health Minister") have since called for legislative reform to allow for swifter reactions to health privacy breaches.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $280.00 (print or PDF)
$425.00 (print & PDF)

Notwithstanding several IPC orders and reports that have made findings regarding these violations of patient privacy, the incidents do not appear to be on the decline. In response to this trend, professional self-regulatory bodies should consider what measures they may be able to take in order to reduce the occurrence of unauthorized access by health professionals to patients' personal health information.

Professional Discipline: *College of Nurses of Ontario v. Marcella Calvano*

The College of Nurses of Ontario has recently disciplined Marcella Calvano, a nurse formerly employed by Sault Area Hospital, who, over a two-year period, viewed the personal health information of 338 patients when she was not authorized to do so.

Ms. Calvano was employed as a critical care nurse in the Intensive Care Unit and emergency department before transferring into surgery in 2010. The hospital's system allowed employees to access information about patients in the emergency department, including date of birth, the primary complaint, lab work/results, and diagnostic imaging results. It became known that Ms. Calvano was accessing the database inappropriately when another nurse attempted to access a patient's electronic health record and could not do so because Ms. Calvano was viewing it. A subsequent audit revealed the extent of Ms. Calvano's health privacy breaches.

The College of Nurses of Ontario referred allegations of professional misconduct to the Discipline Committee for a hearing. Ms. Calvano pleaded guilty to committing professional misconduct on the basis that she had contravened a standard of practice of the profession and engaged in dishonourable and unprofessional conduct by accessing the personal health information of clients without consent or other authorization.

The Discipline Committee imposed a penalty that recognized the seriousness of the conduct. The Discipline Committee ordered that Ms. Calvano's certificate of registration be suspended for three months, that she be required to appear before the panel to be reprimanded, and that the following terms, conditions, and limitations be imposed on her certificate of registration: that she (1) must successfully complete specified remedial activities; (2) must inform employer(s) of results of the discipline hearing; and (3) must inform the College of Nurses of Ontario of all nursing employer(s) for a period.[2]

This case is but one in a collection of health privacy cases that are coming before regulatory bodies. Unauthorized access cases are also finding their way to the courts. Most recently, criminal and quasi-criminal charges were laid by the Ontario Securities Commission, following its investigation relating to the misuse of confidential patient information from the Rouge Valley Health System and the Scarborough Hospital.

First Prosecution under *PHIPA*

Currently, in order to prosecute a person for a privacy breach, the IPC must refer the matter to the Attorney General, as only the Attorney General may commence a prosecution under *PHIPA*. The first prosecution under *PHIPA* was brought against a nurse formerly employed at North Bay Regional Health Centre. It was alleged that she improperly accessed 5,804 patient health records over a seven-year period. The nurse was charged with nine counts of willfully collecting and using personal health information without authority in contravention of s. 72(1)(a) of *PHIPA*.

The nurse brought *Canadian Charter of Rights and Freedoms* ("Charter") applications pursuant to s. 11(b) for unreasonable delay and s. 7 for abuse of process and selective prosecution. Justice of the Peace Lauren Scully dismissed the s. 7 argument but found that the Crown's delay was in violation of s. 11(b) of the Charter, and, therefore, a stay of the action was ordered.[3]

Since then, the IPC has referred three additional cases involving unauthorized access by health professionals to patient medical records.

Given the growing number of incidents of unauthorized access, both the IPC and Health Minister Eric Hoskins have called for more vigorous action to be taken regarding privacy violations. The IPC has advocated for legislative reform so that the IPC would run its own investigations and no longer need the approval of the Attorney General to prosecute. On June 10, 2015, Minister Hoskins announced his intention to introduce amendments to *PHIPA* that include mandatory reporting of privacy breaches to the IPC and, in certain cases, to relevant regulatory colleges; doubling the maximum fine for offences from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for organizations; eliminating the requirement that a prosecution be launched within six months of the alleged privacy breach; and clarifying the authority under which health care providers may collect, use, and disclose personal health information in electronic health records.

Recommendations for Professional Self-Regulatory Bodies

Expectations that a health professional will retain confidentiality of patient health information have

always been fundamental to the standards of professional practice. With electronic records, there are unique and increased privacy risks. As noted, unauthorized access to patients' personal health information appears to be a growing problem. It is therefore important for professional self-regulatory bodies to consider what steps they can take to address the issue of privacy breaches by regulated health professionals.

Regulatory bodies should consider mechanisms to educate their members on the importance of protecting patients' personal health information and on the negative impact privacy breaches have on patient care. For example, health privacy violations may deter patients from seeking testing or treatment, or cause patients to withhold or falsify personal health information for fear of unauthorized access to this sensitive information. In the event patients learn they have been the victim of a breach, they may suffer emotional or psychological stress, compounded by the fact that they may be experiencing a serious or life-threatening illness at the time. Patients may also face discrimination and stigmatization as a result of a privacy violation. Continuing occurrences of privacy breaches may also result in a serious loss of trust and confidence in the health system.

Regulatory bodies should also educate their members about the significant consequences that await health professionals found violating the confidentiality of patient health information. In addition to discipline proceedings by regulatory bodies, potential consequences to health professionals are loss of employment, difficulty in regaining employment, damage to reputation, investigation by the IPC, prosecution and fines under *PHIPA*, and other legal action such as tort actions for breach of privacy.

In addition to educating their members, regulatory bodies should consider developing specific practice standards or guidelines on confidentiality and privacy of personal health information (if they do not already have them). Regulatory bodies should also provide additional orientation and training to their screening and discipline committees regarding the significant impact privacy breaches have on patients and patient care. Lastly, regulators should ensure penalties imposed for health privacy breaches at disciplinary proceedings recognize the seriousness of the conduct and are effective in deterring members from engaging in similar conduct.
While members found guilty of unauthorized access to personal health information face consequences outside of the regulatory sphere, regulatory bodies can certainly play a role in the effort to reduce the occurrence of privacy breaches by health professionals.

---

1 S.O. 2004, c. 3, Schedule A.

2 The information regarding the penalty, ordered by the Discipline Committee, is based on the public register of the College of Nurses of Ontario. At the time of publication of this article, the decision of the Discipline Committee was not yet publicly available.

3 Discipline proceedings by the College of Nurses of Ontario, respecting allegations of professional misconduct on the part of this nurse, are pending.