Aug 16, 2015

The Perils of Privacy Breaches by Hospital Employees

Author(s): Rhonda Shirreff, Sunny Khaira

Canadian privacy laws contain a basic safeguarding principle: access to personal information may only be granted on a need-to-know basis. Snooping violates that principle.

Several Ontario arbitrators have upheld a “zero tolerance” approach for privacy breaches at hospitals, holding that summary dismissal is the appropriate remedy for deliberate breaches of confidentiality and workplace codes of conduct by hospital employees who snoop into patient records for their own reasons, rather than for any legitimate purpose.

For example, in North Bay Health Centre v. O.N.A., (2012) 216 LAC (4th) 38, a 12-year employee with a good record was fired for violating patient privacy after she accessed 5,804 individual patient health records and made over 12,000 unauthorized inquiries over a seven-year period. The arbitrator found the sheer volume of the violations warranted dismissal, adding that the employee knew or should have known that her access to patient records was properly limited to those she had a professional obligation to care for.

Arbitrators have upheld the zero tolerance approach even when hospital employees’ snooping was much less pervasive. In Bluewater Health and O.N.A. (Hardy) (Re), 2010 CLB 33129, an arbitrator upheld the termination of a part-time nurse for accessing the medical records of four patients who were not under her care. Although the nurse’s unauthorized access to each patient’s record lasted for only a few seconds, the arbitrator found it difficult to accept that it was accidental. In Timmins & District Hospital and O.N.A. (Peever), (2011) 208 LAC (4d) 43, an arbitrator upheld the termination of a 22-year employee who accessed the clinical mental health records of a patient who was married to her son. The arbitrator rejected the employee’s claim that she was unaware her conduct violated the hospital’s ethics and confidentiality policies. As the employee showed no remorse and there was no assurance that she would not snoop into patient records again, the arbitrator concluded there were no compelling circumstances to mitigate her discharge.

Arbitrators will deviate from the zero tolerance approach in the face of compelling mitigating circumstances. For example, Vancouver Coastal Health Authority and HAS BC (Gamache) (Re), (2014) 118 CLAS 104, involved a 24-year employee who was fired after improperly accessing a patient’s medical records and emailing that information to a friend whose sister – unbeknownst to the employee – had recently separated from the patient. The arbitrator found “extremely compelling” circumstances to
substitute a 3-month unpaid suspension for the termination, including the employee’s strong employment record, her candid and sincere admission of wrongdoing, the fact that her wrongdoing was isolated and out of character, and the stressors in her life at the time, including her husband recently being diagnosed with melanoma and an aging mother with serious medical set-backs.

Moreover, a zero tolerance approach to hospital employee snooping may not be sufficient for hospitals to ward off civil liability for patient privacy breaches, as the following case demonstrates.

In 2011, the Peterborough Regional Health Centre discovered that a number of employees, including a supervising nurse, had accessed the personal health information of up to 280 patients without their advance knowledge or consent. Based on media reports, the breach included unauthorized access to the records of a victim of domestic violence who was in hiding, plus unauthorized access to hundreds of therapeutic abortion files by a records clerk who was an anti-abortion activist. The Health Centre took prompt remedial action. It fired the employees involved, conducted a hospital-wide privacy campaign and, as required by the Ontario Personal Health Information Protection Act (PHIPA), notified the affected patients of the privacy breach. The Ontario Information and Privacy Commissioner conducted an investigation. He found that the Health Centre had “responded reasonably” to the privacy breaches and determined that “no further action was warranted” against the Health Centre.

Unsatisfied with the outcome of the Commissioner’s investigation, a group of affected patients launched a class action against the Health Centre, seeking over $5 million in damages for the unauthorized access to their personal health information. In February 2015, the Ontario Court of Appeal held that it was permissible to bring a class proceeding for civil damages against the Health Centre for the unauthorized access to patient records, even though the Commissioner had already conducted an investigation under PHIPA [Hopkins v. Kay, 2015 ONCA 112].

The aftermath of the privacy breaches at the Peterborough Regional Health Centre suggests that hospitals could be liable for significant civil damages, even when they have taken a zero tolerance approach to employees improperly accessing patient records and have responded reasonably under PHIPA. As the class action law suit moves forward, it will serve as an important reminder of the potential ramifications of confidentiality breaches by snooping hospital employees.

This article originally appeared in Hospital News.

© Osler, Hoskin & Harcourt LLP. This content is for general information purposes only and does not constitute legal or other professional advice or an opinion of any kind. You can subscribe to receive updates on a range of industry topics at osler.com/subscribe.