SNOOPING INTO MEDICAL RECORDS

IAPP PRIVACY SYMPOSIUM

- May 28, 2015 -

Manuela Di Re, Director of Legal Services

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

The Promise of Electronic Records

- Potential to facilitate more efficient and effective health care and improve the quality of health care provided
- Accessible by all health care providers involved in the health care of an individual, regardless of location
- More complete than paper records which tend to be spread over a wide range of health care providers
- Easier to read and locate than paper records
- Can be designed to enhance privacy, e.g. through access controls, audit logs and strong encryption

The Peril of Electronic Records

- If privacy is not built into their design and implementation, electronic records pose unique risks to privacy
- Allow for the collection, use and disclosure of large amounts of personal health information from diverse sources
- May be more quickly and easily linked and used for ever increasing and undefined purposes
- May attract hackers and others with malicious intent
- Increases the risk of authorized individuals accessing personal health information for unauthorized purposes

Unauthorized Access by Authorized Individuals

- Resources are often spent defending against external attacks, however, internal threats are also a great risk

- In *Investigation Report H-2010-001*, the former Information and Privacy Commissioner of Saskatchewan stated:

  While there has been a lot of attention to the risk that some outsider may attempt to compromise the relatively elaborate technical safeguards and security features attached to electronic health record domain repositories, there has been much less attention paid to the more likely risks posed by the carelessness of trustee organizations and the curiosity of their employees and contractors.

Sanctions for Unauthorized Access

- Investigation by privacy oversight bodies
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

Alberta

Prosecution in 2007

- A medical office clerk plead guilty and was fined $10,000 under the *Health Information Act*
- Accessed the information of the wife of a man with whom she was having an affair using Alberta Netcare and fax
- Accessed the information on six different occasions

Investigation Report H2011-IR-004

- Physician used Alberta Netcare to access records of a partner's former spouse and mother and girlfriend of the former spouse
- Used the accounts of colleagues who failed to log out
- Accessed records on 21 occasions over a period of 15 months

Alberta

Prosecution in 2011

- A pharmacist plead guilty and was fined $15,000 under the *Health Information Act*
- Used Alberta Netcare to access the records of a number of women who attended her church and posted the prescription information of some of the women on Facebook

Prosecution in 2014

- A medical laboratory assistant received a four month conditional sentence, eight months probation and a $500 fine
- Accessed the personal health information of 34 individuals and uttered forged documents under the *Criminal Code*

Saskatchewan

Investigation Report H-2010-001

- Pharmacist used the Pharmaceutical Information Program, a domain repository in Saskatchewan's electronic health record, to access drug profiles of three individuals on nine occasions after a business arrangement with the individuals dissolved

Investigation Report H-2013-001

- Employees of Regina Qu'Appelle Regional Health Authority accessed their own health information, accessed and modified the health information of other employees and accessed the health information of other individuals

Manitoba

Report 2011-0513 and 2011-0514

- An employee of CancerCare Manitoba accessed the electronic medical record of a child of an acquaintance
- The employee accessed three tabs – patient notes, agenda and summary – for two minutes two seconds
- Because the record was created earlier that day, the employee was only able to access the name and cancer registry number

Ontario

Order HO-002

- A registered nurse accessed the records of the estranged spouse of her boyfriend
- The records were accessed over a six-week period

Order HO-010

- A diagnostic imaging technologist accessed the records of the current spouse of her former spouse
- The records were accessed on six occasions over nine months

Order HO-013

- Two employees accessed records to market and sell RESPs

Newfoundland and Labrador

Prosecution in September 2014

- An employee of Western Health plead guilty and was fined $5000 under the *Personal Health Information Act*
- Accessed personal health information for unauthorized purposes on 75 occasions within a span of less than one month

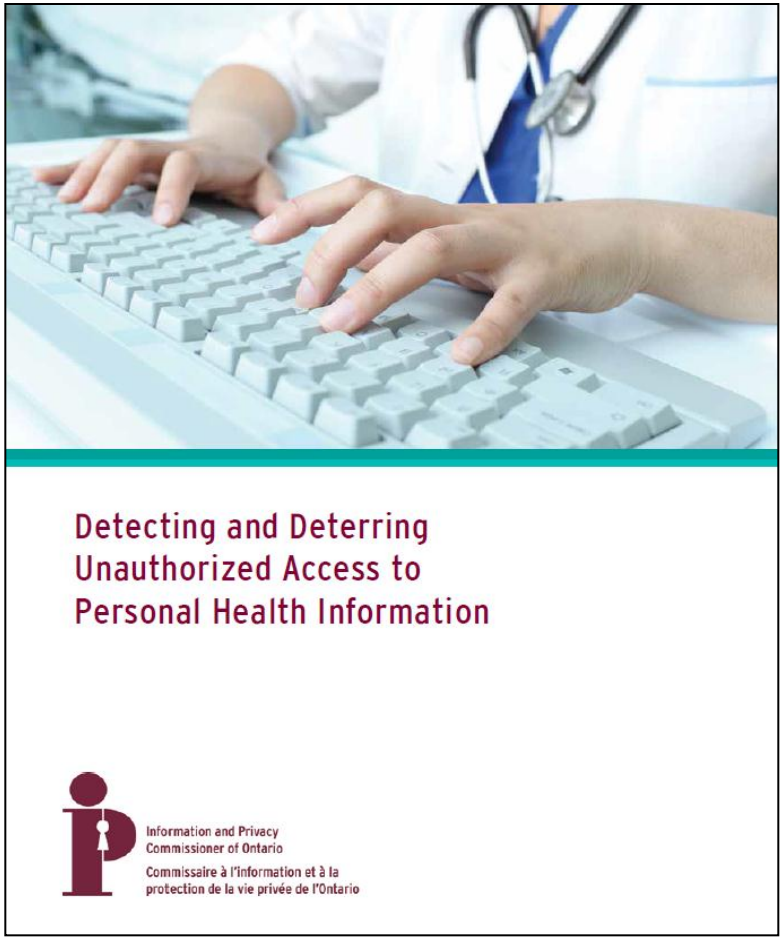
Prosecution in October 2014

- A nurse employed by Eastern Health was found guilty and fined $1000 under the *Personal Health Information Act*
- Accessed personal health information for unauthorized purposes on 18 occasions over a one year period

How to Reduce the Risk…

- Clearly articulate the purposes for which employees, staff and other agents may access personal health information
- Provide ongoing training and use multiple means of raising awareness such as:
  - Confidentiality and end-user agreements
  - Privacy notices and privacy warning flags
- Immediately terminate access pending an investigation
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information
- Impose appropriate discipline for unauthorized access

New Guidance Document: Detecting and Deterring Unauthorized Access



- Impact of unauthorized access
- Reducing the risk through:
  - ✓ Policies and procedures
  - ✓ Training and awareness
  - ✓ Privacy notices and warning flags
  - ✓ Confidentiality and end-user agreements
  - ✓ Access management
  - ✓ Logging, auditing and monitoring
  - ✓ Privacy breach management
  - ✓ Discipline

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca