UNAUTHORIZED ACCESS

Manuela Di Re

Director of Legal Services and General Counsel
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

OSGOODE PROFESSIONAL DEVELOPMENT

April 9, 2019

Meaning of Unauthorized Access

- Unauthorized access is when you view, handle or otherwise deal with personal health information without consent and for purposes not permitted by the *Personal Health Information Protection Act* (*PHIPA*)
- For example:
  - When you are not providing health care to the individual
  - When the individual has provided an express instruction
  - When it is not necessary for your employment, contractual or other responsibilities
- The act of viewing the personal health information on its own, without any further action, **is** an unauthorized access
- Unauthorized access is a serious matter, regardless of the motive

Education and Quality Improvement

- There are a number of provisions in *PHIPA* that permit you to use personal health information without consent, including:
  - For risk and error management
  - To improve or maintain the quality of care and related programs or services
  - For educating agents to provide health care
- There have been a number of instances where custodians or agents have accessed personal health information claiming it was for one of these purposes

Challenges in Establishing "Unauthorized" Access

- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
  - Have policies that set out the purposes for which access is permitted and not permitted in relation to risk management, quality improvement and education
  - Have procedures that must be followed when accessing personal health information for these purposes
  - Inform agents when access is permitted and is not permitted, through training, notices, flags in electronic systems, agreements, etc.

How to Address Challenges

- Clearly articulate the purposes for which agents may access personal health information
- Implement a policy that sets out whether and in what circumstances an agent is permitted to access information for risk and error management, quality improvement and education
- The policy should require:
  - Agents to obtain written authorization prior to accessing information for these purposes
  - That the written authorization set out, at a minimum:
    - ✓ The specific circumstances and particular risk or error management activity(ies), quality improvement activity(ies) and educational purpose(s) for which the personal health information may be accessed
    - ✓ Any conditions, restrictions, and limitations imposed on the access

How to Address Challenges

- 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
- Impose appropriate discipline for unauthorized access
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information

Logging, Auditing and Monitoring

- Big data analytics and artificial intelligence are being used to deter, detect and prevent unauthorized access
- In collaboration with Mackenzie Innovation Institute (Mi2), Michael Garron Hospital, Markham Stouffville Hospital, and vendor KI Design, Mackenzie Health began a Privacy Auditing Innovation Procurement project
- The Information and Privacy Commissioner of Ontario (IPC) participated on the steering committee to provide a regulator perspective

Results of Pilot

- The solution used big data analytics and artificial intelligence to determine what accesses could be explained
- A small portion of unexplained accesses were flagged for further investigation
- During the six month pilot, many privacy breaches were detected
- The number of breaches decreased significantly as the solution was fine tuned and missing information from various information systems (e.g., scheduling) was added
- The number of breaches is expected to decrease further with staff awareness and increased ability for solution to explain accesses

Guidance Document

Reduce 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

Detecting and Deterring Unauthorized Access to Personal Health Information

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

Consequences of Unauthorized Access

- Duty to notify
- Review or investigation by the IPC
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

Duty to Notify

Notification of Individual

- A custodian must notify the individual at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority
- In the provincial electronic health record, the custodian must also notify the individual at the first reasonable opportunity if it is collected without authority

Notification of the IPC

- A custodian must also notify the IPC of a theft, loss or unauthorized collection, use or disclosure in the circumstances set out in section 6.3 of the Regulation to *PHIPA*

Reviews and Investigations by the IPC

- A final order of the IPC may be filed with the court and on filing, is enforceable as an order of the court
- The IPC has issued orders involving unauthorized access, including:

HO-002

- A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care over six-weeks during divorce proceedings

HO-010

- A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care on six occasions over nine months

HO-013

- Two employees accessed records to market and sell RESPs

Offences

- It is an offence to wilfully collect, use or disclose personal health information in contravention of *PHIPA*
- Consent of the Attorney General is required to commence a prosecution for offences under *PHIPA*
- On conviction, an individual may be liable to a fine of up to $100 000 and a corporation of up to $500 000

Prosecutions

To date, five individuals have been successfully prosecuted:

- **2016** – two radiation therapists at a Toronto Hospital
- **2016** – a registration clerk at a regional hospital
- **2017** – a social worker at a family health team*
- **2017** – an administrative support clerk at a Toronto hospital

*The fine in this case is the highest fine to date for a health privacy breach in Canada - the social worker was ordered to pay a $20 000 fine plus a $5 000 victim surcharge

"The various victims have provided victim impact statements which are quite telling in terms of the sense of violation, the loss of trust, the loss of faith in their own health care community, and the utter disrespect [the accused] displayed towards these individuals."

"I have to take [the effect of deterrence on the accused] into consideration, but realistically, it's general deterrence, and that has to deal with every other heath care professional or someone who is governed by this piece of legislation. This is an important piece of legislation …"

- Justice of the Peace, Anna Hampson

Statutory or Common Law Actions

- A person affected by a final order of the IPC or by conduct that gave rise to a final conviction for an offence may start a proceeding for damages for actual harm suffered
- Where the harm was caused wilfully or recklessly, the court may award an amount not exceeding $10 000 for mental anguish
- In 2012, the Ontario Court of Appeal recognized a common law cause of action in tort for invasion of privacy called “intrusion upon seclusion”

Discipline by Regulatory Colleges

- The Masters of Social Work student prosecuted was also disciplined by the Ontario College of Social Workers and Social Service Workers in June 2017
- The member admitted and the panel found that the student committed professional misconduct, including by undermining the "trust the public has in social workers and other health care providers"
- The member was reprimanded, her certificate of registration was suspended for six months and she was required to complete an ethics course
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- The member accessed the health records of a colleague through the hospital electronic records system without authorization
- The relationship between the member and the colleague was deteriorating and the member questioned the well being and mental health of the colleague
- The member admitted that he engaged in professional misconduct
- The member's certificate of registration was suspended for three months and he was required to complete an individualized instruction in medical ethics
- The member was also ordered to pay costs of $5 000 to the College

Discipline by Regulatory Colleges

- The member accessed the health records of a patient through the hospital electronic records system without authorization
- The patient's admission and general diagnosis were widely publicized and a privacy notice popped up when the patient's name was clicked in the system
- The member admitted her actions and claimed that she was curious about the patient's age
- The member's certificate of registration was suspended for one month and a number of terms, conditions and limitations were placed on her certificate of registration, including to notify employers of this decision for a 12 month period

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

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965