Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

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

Custodians should maintain this information to ensure they are ready to report on the 2018 calendar year in early 2019:

STOLEN PERSONAL HEALTH INFORMATION

- Total number of incidents where personal health information was stolen
- Of the total in this category, the number of incidents where:
  - theft was by an internal party (such as an employee, affiliated health practitioner or electronic service provider)
  - theft was by a stranger
  - theft was the result of a ransomware attack
  - theft was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB keys or laptops) was stolen
  - paper records were stolen
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

LOST PERSONAL HEALTH INFORMATION

- Total number of incidents where personal health information was lost
- Of the total in this category, the number of incidents where:
  - loss was a result of a ransomware attack
  - loss was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB keys or laptops) was lost
  - paper records were lost
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected

- 51 to 100 individuals were affected
- over 100 individuals were affected

USED WITHOUT AUTHORITY

- Total number of incidents where personal health information was used (e.g. viewed, handled) without authority
- Of the total in this category, the number of incidents where:
  - unauthorized use was through electronic systems
  - unauthorized use was through paper records
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

DISCLOSED WITHOUT AUTHORITY

- Total number of incidents where personal health information was disclosed without authority
- Of the total in this category, the number of incidents where:
  - unauthorized disclosure was through misdirected faxes
  - unauthorized disclosure was through misdirected emails
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

NOTES:

Do not count each incident more than once. If one incident includes more than one of the above categories, choose the category that it best fits. For example, if an employee accessed personal health information without authority, and then disclosed the information, count that incident as either a use or a disclosure, but not both.

In this annual statistics report, you must include all thefts, losses, or unauthorized uses or disclosures, even if you were not required to report them to the IPC under Section 6.3 of the Regulation.

Health privacy breach statistics will be collected through the IPC's Online Statistics Submission Website in early 2019. Custodians will find it easier to provide the IPC with the information required at that time if they keep track of these statistics over the course of 2018.

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