Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 175

HI19-00007

A Group of Medical Clinics and Related Entities

March 25, 2022

Summary: This investigation file was opened following the publication of a Toronto Star article in 2019 (the Article). The Article reported that a company that sells and supports electronic medical record software in primary care practices in Ontario, was anonymizing health data and selling the data to a third party corporation. In response to the article, the Office of the Information and Privacy Commissioner of Ontario commenced a review under the *Personal Health Information Protection Act* (the *Act*) and sought to identify the individual or entity who allegedly de-identified and sold the data.

The corporation that was identified as having sold the information was named as a respondent in this investigation and a number of other respondents were also added, one of which was identified as the health information custodian.

This Decision concludes that the act or process of de-identifying personal health information is a "use" within the meaning of section 2 of the *Act,* and that the use of personal health information for the purpose of de-identification is permitted without the consent of the individual, where the conditions set out under subsection 37(1)(f) of the *Act* are met. At the time of this investigation, the health information custodian's written public statement about its information practices did not comply with section 16(1)(a) of the *Act*. However, this issue has since been remedied and the custodian's updated privacy policy now meets the requirements of the *Act* by explicitly describing its practice of de-identifying personal health information and selling the information to a third party for a number of purposes, including for health-related research. With regard to the de-identified personal health information, the custodian has complied with subsection 12(1) of the *Act*, in that reasonable steps have now been taken to ensure the protection of personal health information by amending the sale agreement to include additional privacy and security controls.

Further, the IPC has no information to suggest that the personal health information was not properly de-identified within the meaning of the *Act*.

Accordingly, this review will be concluded without proceeding to the adjudication stage and without an order being issued by this office.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 1(a), 1(e), 2, 3(1), 4(1), 10(1), 12(1), 16(1)(a), 18, 29, 37(1)(f), 37(2).

Decisions considered: HO-010.

BACKGROUND:

[1] This investigation file was opened following the publication of a Toronto Star article in 2019 (the Article).

[2] The Article reported that a company that sells and supports electronic medical record (EMR) software in primary care practices in Ontario, was anonymizing health data and selling the data to a third party corporation.

[3] On February 21, 2019, the Office of the Information and Privacy Commissioner of Ontario (the IPC) commenced a review under the *Personal Health Information Protection Act, 2004* (*PHIPA* or the *Act*), and sought to identify the individual or entity who allegedly de-identified and sold the data.

[4] The corporation that was identified as having sold the information was subsequently named as a respondent in this investigation.

[5] During this investigation, the respondents explained that the personal health information that was de-identified and sold was obtained from several medical clinics related to the named respondent. Subsequently, several related entities were added as respondents in this investigation. The respondents identified one of them as the health information custodian (the custodian) of the personal health information that was de-identified and sold. The respondents also explained that the information was sold by a related entity acting as the agent of the custodian for the purpose of entering into a sale agreement with the data purchaser dated March 1, 2013 (the Sale Agreement).

[6] The respondents further advised that one of the named respondents acted as a service provider and/or agent to the custodian by de-identifying the personal health information pursuant to the custodian's instructions and only for the purposes of the custodian.

[7] Regarding the de-identification process and whether this was a "use" of personal health information within the meaning of the *Act*, the respondents took the position that de-identification is not a use of personal health information and that de-identified information falls outside the scope of the application of privacy laws. The respondents

further advised that the custodian's privacy policy informed individuals that their personal health information may be used by the custodian for research, statistics and where permitted or required by law.

[8] The respondents provided submissions relating to the process of de-identifying the personal health information, including details regarding the de-identification protocol implemented and two re-identification risk analyses reports. The respondents advised that a third party conducted the re-identification risk analyses of the information at issue and that the third party concluded that the risk of re-identification was very small.

[9] In the course of this investigation, the respondents took the steps of amending the custodian's privacy policy and the Sale Agreement. The Sale Agreement was amended and re-executed on March 1, 2021 (the Amended Sale Agreement).

[10] The information received from the respondents, as well as my findings with respect to the issues in this investigation, are set out below.

Discussion:

[11] Based on the information provided by the respondents and over which there is no dispute, I find that the custodian identified by the respondents is a "health information custodian" under paragraph 1 of section 3(1) of the *Act*, and that the information at issue constitutes "personal health information" under subsection 4(1) of the *Act* in the custody or control of the custodian. I further find based on submissions provided by the respondents that the information at issue was de-identified by one of the respondents acting as an agent and electronic service provider to the custodian within the meaning of subsection 2, 17 and 10(4) of the *Act* on behalf of, and with the authorization of, the custodian.

[12] In this decision, the following issues will be discussed:

- Is the de-identification of personal health information a "use" under the *Act*?
- If the answer to Issue 1 is yes, is the use of personal health information for the purpose of de-identification permitted under the *Act*?
- Did the custodian's written public statement about its information practices comply with the *Act?*
- Did the custodian take reasonable steps to protect the personal health information at issue in this matter?
- Should this matter proceed to adjudication at the IPC, where a potential order may be issued?

Issue 1: Is de-identification of personal health information a "use" under the *Act*?

[13] Section 2 of the *Act* defines the term "use" in relation to personal health information in the custody or under the control of a custodian or a person, as "to view, handle or otherwise deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning".

[14] At the outset of this investigation, the respondents took the position that the de-identification of personal health information is not a use under the *Act*. The respondents advised that such an interpretation would appear to contradict IPC guidance documents[1] and other material on secondary use of health data,[2] that de-identified information falls outside the scope of privacy legislation, and that obtaining consent would often be impractical or impossible. For instance, the respondents cited IPC guidance published in 2011, entitled, "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy" which provides:

> …[S]ection 37(1)(f) of *PHIPA* specifically states that health information custodians may use personal health information about an individual for the purpose of disposing of or modifying the information in order to conceal the identity of the individual. Therefore, health information custodians not only have an obligation to de-identify personal health information, to the greatest extent possible, but they also have the legal authority to use personal health information for the purpose of de-identification. Once de-identified, in a manner such that it falls outside the scope of *PHIPA*, the information may then be used and disclosed for secondary purposes, without the consent of the individual.[3]

[15] In addition, the respondents advised that if de-identified information were to be treated in the same manner as personal health information under the *Act*, there may be less incentive for custodians to de-identify personal health information and this in turn would be detrimental to the public interest as there would be a reduction of available valuable health information for research purposes. The respondents also advised that hospitals and other public sector organizations regularly transfer, license or sell de-identified information and do not treat it as a "use" of personal health information for which consent of the individual is required.

---

[1] The respondents cited: IPC's "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy" (June 2011); IPC's "De-Identification Guidelines for Structured Data" (June 2016); IPC's "De-Identification Protocols: Essentials for Protecting Privacy" (June 2014); IPC's "A Positive-Sum Paradigm in Action in the Health Sector" (March 2010); IPC's "The Unintended Consequences of Privacy Paternalism" (March 2015).

[2] Patricia Kosseim and Megan Brady, "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes", 2008 CanLIIDocs 5.

[3] IPC's "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy" (June 2011) at page 12.

[16] Subsequent to the receipt of the above response, the respondents further advised that it is unclear whether the act of de-identifying personal health information is a use under the *Act*.

The IPC's Finding

[17] For the reasons that follow, I find that the act or process of de-identifying personal health information is a "use" within the meaning of section 2 of the *Act*.

[18] The modern approach to statutory interpretation cited by the Supreme Court of Canada in *Bell ExpressVu Limited Partnership v. Rex*, 2002 SCC 42 (CanLII) at para. 26 and *TELUS Communications Inc. v. Wellman*, 2019 SCC 19 (CanLII) at para. 47, is set out in Elmer Driedger's text on *Construction of Statutes* (2nd ed. 1983), which provides that:

> [T]he words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament".

[19] Subsection 64(1) of *the Legislation Act, 2006* also applies to the interpretation of an Ontario statute. This subsection requires that the legislation be given "such fair, large and liberal interpretation as best ensures the attainment of its objects."

[20] The term "use" is broadly defined under the *Act* as including "to view, handle or otherwise deal with the information". This broad definition is consistent with the scheme and object of the *Act* and there is no reason to indicate that the provincial Parliament did not intend to ascribe such broad meaning to the term "use" as set out under section 2 of the *Act*. The objects of the *Act* can be derived from the purpose provision under section 1 of the *Act* that includes among its purposes:

> a) to establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care;
>
> […]
>
> e) to provide effective remedies for contraventions of this Act.

[21] Moreover, it is highly telling that among the uses explicitly permitted under subsection 37(1) of the *Act* is to use personal health information "(f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual". Part II of the *Act* sets out the required practices for protecting personal health information.

[22] I am not persuaded by the respondents' submissions that the de-identification of

personal health information is not a use under the *Act* and that so finding would be burdensome on custodians and detrimental to the public interest. The respondents' submissions also appear to conflate the application of the *Act* to information that has been properly de-identified with the actual process or act of de-identifying personal health information.

[23] In support of their position, the respondents relied on the IPC's guidance identified above. However, nowhere in any of the IPC guidance documents relied upon does it state that the *Act* does not apply to the act or process of dealing with or handling personal health information for the purpose of de-identifying it. To the contrary, the IPC's guidance points to subsection 37(1)(f) of the *Act* which "specifically states that custodians may use personal health information about an individual for the purpose of disposing of *or modifying the information in order to conceal the identity of the individual*" (emphasis added).

[24] Finally, it is not relevant to this investigation whether other custodians "regularly transfer, license or sell de-identified information and do not treat it as a "use" of personal health information". If other custodians are using personal health information in contravention of the *Act*, this does not serve to determine whether the respondents have complied with their obligations under the *Act*. The conduct or actions of any other person not named in this investigation is not before me in this matter.

[25] I find that the act or process of de-identifying personal information requires the dealing with or handling of personal health information in order to modify it in such a way so as to conceal the identity of individuals. Including this act or process within the meaning of "use" under the *Act* ensures the protection of privacy of individuals in respect of their personal health information while custodians are engaged in the act or process of de-identifying personal health information. This finding is in line with the public interest of ensuring personal health information is protected at every stage of dealing with and handling personal health information by custodians.

[26] There is no reason or submission before me that justifies not affording the protections set out under the *Act* to personal health information while it is being handled or dealt with during the process of rendering it de-identified. If such was not the case, it would lead to a number of unintended results that would not be aligned with the purposes of the *Act*. For example, a custodian would not be held accountable if reasonable steps were not taken to ensure that the personal health information being de-identified is protected from "theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal" during the de-identification process.[4] Or, a custodian might

[4] Subsection 12(1) of the *Personal Health Information Protection Act, 2004* (*PHIPA)* requires a custodian to "take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal".

escape responsibility by not informing individuals of its use of personal health information for the purpose of de-identification which in turn leaves individuals without the ability to complain about this use to the IPC and seek effective remedy where the individual has reasonable grounds to believe that there has been a contravention or potential contravention of the *Act*, including by the third party recipient who may attempt to re-identify the information and use or disclose it for a purpose not permitted by law.

[27] These would not be the intended consequences of the *Act* based on its purpose at subsection 1(a) to "establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information", the grammatical and ordinary meaning of the term "use" as defined under the *Act,* the security requirements under subsection 12(1) of the *Act*, and the permitted use provision under subsection 37(1)(f) of the *Act*. These unintended results would also, contrary to the *Act's* purpose at section 1(e), deny effective remedies for contraventions of the *Act* in accordance with the complaint provisions, the Commissioner's order making powers and the offence provisions at sections 56, 58, 61 and 72 of the *Act*, respectively.

[28] Consistent with the scheme and object of the *Act*, and the intention of the legislature, I therefore find that the act or process of de-identifying personal health information is a "use" within the meaning of section 2 of the *Act*. Since I have found that the act or process of de-identifying personal health information is a use within the meaning of section 2 of the *Act*, I now turn to the question of whether this use is permissible under the *Act*.

Issue 2: Is the use of personal health information for the purpose of de-identification permitted under the *Act*?

[29] Section 29 of the *Act* prohibits a custodian from using personal health information of an individual unless it has the individual's consent (and is necessary for a lawful purpose), or the use is permitted or required by the *Act*.

[30] Subsection 37(1)(f) of the *Act* permits a custodian to use personal health information without the consent of the individual "in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual". Further, subsection 37(2) of the *Act* permits a custodian to provide the personal health information to an agent who may use it on their behalf for the same purposes permitted under subsection 37(1) of the *Act*.

[31] The respondents advised that to the extent that the de-identification of personal health information is a "use" under the *Act*, it is a use that a custodian may make of the personal health information without obtaining consent of the individual pursuant to subsection 37(1)(f) of the *Act,* and that an agent of the custodian may also use personal health information for this purpose on behalf of the custodian. The respondents further advised that once the information is de-identified, the *Act* does not and cannot apply to

the disclosure or sale of de-identified information.

[32] The respondents submitted that the IPC is not permitted to attempt to change or alter the law by adopting a new and different interpretation in the context of an investigation. The respondents relied on *Ontario (College of Physicians and Surgeons of Ontario) v. Kunynets*, 2019 ONSC 4300 at para. 44 and *Tran v. Canada (Public Safety and Emergency Prepardeness)*, 2017 SCC 50 at para. 44, for the proposition that there is a presumption against retrospectivity and that legislation operates from the day it comes into force.

[33] The respondents advised that the current state of the law is that personal health information may be used by a custodian to generate de-identified information that can be used, disclosed and sold without the consent of the individual, and that de-identified information falls outside the requirements of the *Act*. The respondents expressed concern about being held to a standard not required by law nor even clearly stated in the IPC's non-binding guidelines.

[34] The respondents were asked to make submissions on the meaning of the phrase "in a manner consistent with Part II" under subsection 37(1)(f) of the *Act*, how this phrase impacts or affects any permissible use under this subsection and whether the respondents' use of the personal health information was in a manner that is consistent with Part II of the *Act*. In response, the respondents advised that the modification of personal health information in order to de-identify it, is consistent with Part II of the *Act* in that the de-identification protocols used ensure accuracy, security of the information, and the handling of the records in a secure manner. The respondents advised that given subsection 37(1)(f) relates to the destruction and modification of personal health information, the most relevant provision of Part II of the *Act* would be section 13. Specifically, subsection 13(1) of the *Act* provides:

> Handling of records
>
> 13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

[35] The respondents further advised that the requirement for a written public statement under section 16, also found in Part II of the *Act*, has been addressed, as will be further elaborated below.

[36] The respondents also submitted that since they take the position that the *Act* does not apply to the de-identification of personal health information, the consent of individuals was not required for the use of the personal health information pursuant to section 29 of the *Act*. In the alternative, the respondents took the position that the custodian had the implied consent of individuals to use their personal health information for statistical and

research purposes, which the custodian did by de-identifying the information. I asked the respondents to provide any applicable agreements, consents or authorizations in support of their alternative position and explain how the consent requirements under section 18 in Part II of the *Act* have been met. Subsections 18(1) and 18(5) of the *Act* provide:

> Elements of consent
>
> 18 (1) If this Act or any other Act requires the consent of an individual for the collection, use or disclosure of personal health information by a health information custodian, the consent,
>
> (a) must be a consent of the individual;
>
> (b) must be knowledgeable;
>
> (c) must relate to the information; and
>
> (d) must not be obtained through deception or coercion.
>
> Knowledgeable consent
>
> (5) A consent to the collection, use or disclosure of personal health information about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows,
>
> (a) the purposes of the collection, use or disclosure, as the case may be; and
>
> (b) that the individual may give or withhold consent.

[37] On the question of compliance with section 18 of the *Act*, the respondents relied on the custodian's privacy policy which informed individuals that their personal health information may be used by the custodian for research, statistics and where permitted or required by law. The respondents advised that the personal health information was de-identified by the custodian for research and statistics and that the custodian had the implied consent of individuals by virtue of the notice provided in the privacy policy. In response to this submission, I further asked the respondents to confirm whether the privacy policy relied upon informed individuals 1) that the custodian may de-identify their personal health information; 2) that the custodian may disclose or sell this information to a third party, and 3) that this third party may in turn use the de-identified information for research or statistical purposes. The respondents confirmed that the privacy policy did not provide such notices to individuals.

The IPC's Finding

Permitted use without consent

[38] I find that the use of personal health information for the purpose of de-identification is a permitted use without the consent of the individual where the conditions set out under subsection 37(1)(f) of the *Act* are met.

[39] Applying the modern approach to statutory interpretation set out above, subsection 37(1)(f) permits the use of personal health information to de-identify the information in a manner that is consistent with Part II of the *Act*. Section 37(1)(f) specifically refers to the modification of personal health information in order to conceal the identity of the individual. The term "modify" is used in a number of provisions in the *Act* but is not defined. The Oxford dictionary defines "modify" as "to change something slightly, especially in order to make it more suitable for a particular purpose".[5] In order to remove information that identifies the individual, the information would need to be used and modified accordingly.

[40] Interpreting subsection 37(1)(f) to permit the de-identification of personal health information in a manner that is consistent with Part II of the *Act* is supported by the definition of "de-identify" in section 2 of the *Act*, which means "to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual".[6] This interpretation is also consistent with the definition of "identifying information" under subsection 4(2) of the *Act*, which means "information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual".

[41] My interpretation of subsection 37(1)(f) of the *Act* is further supported by the objects and scheme of the *Act*. Permitting custodians to use personal health information for the purposes of de-identification assists in advancing the *Act's* overall purpose of establishing rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information.[7] In addition, subsection 37(1)(f) is a provision found under Part IV of the *Act* entitled, "Collection, Use and Disclosure of Personal Health Information" and the heading of this subsection is entitled, "Permitted use".

[42] I do not agree with the respondents that in interpreting the phrase "in a manner

---

[5] Definition of "modify", Oxford Learner's Dictionary: https://www.oxfordlearnersdictionaries.com/definition/english/modify.

[6] The definition of the term "de-identify" was included under *PHIPA* when enacted only with respect to section 47 (disclosure to a health data institute for analysis of health system) until an amendment was made, which came into force on July 31, 2020 by proclamation of the Lieutenant Governor. The definition of the term "de-identify" is now set out under section 2 of *PHIPA* and is identical to the definition previously set out under section 47.

[7] See section 1(a) of *PHIPA*.

consistent with Part II", the most relevant provision is section 13 of the *Act*. While section 13 is relevant in that de-identification may assist a custodian in meeting the requirement to retain, transfer and dispose of personal health information in a secure manner, it is not the only or most relevant provision under Part II of the *Act* for the purpose of this investigation.

[43] I find that the phrase "in a manner consistent with Part II" under subsection 37(1)(f) requires a custodian that uses personal health information for the purpose of de-identification, to use and modify the personal health information in a manner that is consistent with the entirety of Part II of the *Act* which is entitled, "Practices to Protect Personal Health Information". This Part contains provisions related to security, accuracy, handling of records and openness and transparency. Requiring that any non-consensual use and modification of personal health information for the purpose of de-identifying the information must nonetheless be completed in a manner consistent with the entirety of Part II[8], ensures that the privacy of individuals in respect of their personal health information and the confidentiality of that information is protected – a core object of the *Act*.

[44] Where subsection 37(1)(f) is relied upon, the context or facts of a matter may require greater focus or review of certain provisions under Part II of the *Act* as may be relevant. For the purposes of this investigation, it is relevant to determine whether the custodian's written public statement about its information practices complied with the requirements under subsections 16(1)(a) of the *Act* and whether the custodian de-identified the personal health information of individuals in a secure manner in compliance with subsection 12(1) of the *Act*. Both these requirements, found in Part II of the *Act*, will be analyzed further below.

[45] My interpretation of subsection 37(1)(f) of the *Act* and its relation with Part II does not place further restrictions that are not set out in the *Act,* or that are being applied retrospectively. With respect to the respondents' submission that the IPC is not permitted to attempt to change or alter the law in the context of an investigation, it is certainly not the IPC's role to change or alter the law. However, it is the IPC's role to interpret and apply the law to the individual facts of a case, particularly when a fact scenario arises and/or a provision of the *Act* is engaged that has not yet been considered and applied by the IPC.

[46] Regarding the respondents' other submission about not being held to a standard that is not stated in the IPC's non-binding guidelines, the IPC's guidance do not purport to cover every factual circumstance, context and legal requirement that may apply under the *Act*. While IPC guidance documents are intended to explain and simplify certain aspects of the *Act*, the respondents' obligations are derived first and foremost from the *Act* itself.

---

[8] Part II has a broader application, including to other collections, uses and disclosures under the *Act*.

Use with the consent of the individual

[47] Since I have determined that subsection 37(1)(f) of the *Act* permits the use of personal health information *without* the consent of the individual "in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual", there is no need to make a determination on the respondents' alternative submission based on implied consent. However, for the purpose of completeness, I will address the respondent's submission that the custodian's privacy policy which states that the custodian may use personal health information for the purpose of research, statistics and where permitted or required by law, was sufficient for the purpose of obtaining the implied consent of individuals.

[48] In response to my question, the respondents confirmed that the privacy policy did not inform individuals that 1) the custodian may de-identify their personal health information; 2) that the custodian may disclose or sell this information to a third party, and 3) that this third party may in turn use the de-identified information for research or statistical purposes. An individual reading the custodian's privacy policy would not be aware in the least that their personal health information may be used by the custodian for the purpose of de-identification and sale to a third party. By not being made aware of these information practices, the individual would also not be presented with the opportunity to either provide or withhold their consent. For these reasons, it is my view that the respondents cannot meet the knowledgeable consent requirements under subsections 18(1)(b)-(c) and 18(5) of the *Act*.

Issue 3: Did the custodian's written public statement about its information practices comply with the *Act*?

[49] I now return to the first of the two additional questions I identified in paragraph 44 above as being relevant provisions of Part II of the *Act* that must be examined in this case. The first of these is whether the respondents meet the requirements to have in place a written public statement of its information practices as set out in subsection 16(1) of Part II of the *Act*. Subsection 16(1) states:

> 16 (1) A health information custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that,
>
> (a) Provides a general description of the custodian's information practices;
>
> (b) describes how to contact,
>
> (i) the contact person described in subsection 15 (3), if the custodian has one, or
>
> (ii) the custodian, if the custodian does not have that contact person;

> (c) describes how an individual may obtain access to or request correction of a record of personal health information about the individual that is in the custody or control of the custodian; and
>
> (d) describes how to make a complaint to the custodian and to the Commissioner under this Act.

[50] The information practices referred to in subsection 16(1) of the *Act* must be informed by subsections 10(1) and 10(2):

> Information practices
>
> 10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.
>
> Duty to follow practices
>
> (2) A health information custodian shall comply with its information practices.

[51] In turn, section 2 of the *Act* defines "information practices" as follows:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
>
> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[52] During this investigation, I requested the respondents to provide a copy of the custodian's information practices that were in place at the time of the collection and use of the personal health information that was de-identified and sold to the data purchaser. The respondents were also asked whether the custodian had a written public statement that provided a general description of its information practices pursuant to subsection 16(1)(a) of the *Act* at the time of the collection and use of the personal health information that was de-identified and sold to the data purchaser.

[53] In response to the above questions, the respondents relied on the custodian's privacy policy which informed individuals that their personal health information may be used by the custodian for research, statistics and where permitted or required by law. The respondents further advised that while the privacy policy did not explicitly state that

the personal health information would be de-identified and that the de-identified information would be sold, the privacy policy described the intended uses of the personal health information for research and statistical purposes.

[54] The respondents were asked to provide further submissions (if any) on how the custodian's privacy policy's reference to the use of personal health information for research, statistics and for purposes permitted or required by law meets the requirements under subsection 16(1)(a) of the *Act* to describe the respondents' use of personal health information for the purpose of de-identification and sale to a third party. The respondents advised in their response that the *Act* only requires that individuals be informed of the purposes of the collection, use or disclosure of their personal health information.

[55] The respondents also advised that IPC guidance documents do not indicate that a custodian must notify individuals that their personal health information will be de-identified and then disclosed, whether on a remunerated or non-remunerated basis, and that there are no decisions or orders from the IPC that it is aware of that address the "required degree of specificity of notice to patients in the context of de-identifying personal heath information nor the disclosure of such information in the "de-identified" format". The respondents advised that it cannot be held to a higher standard that is not stated in law nor applied to other organizations. Regarding other organizations, the respondents provided a table with listed custodians and noted that, with the exception of one, the privacy policies reviewed do not provide a "specific statement of 'de-identification' of information".

[56] With respect to the custodian's practice of de-identifying personal health information and selling the information to the data purchaser, the respondents were asked to provide the following information:

- the overall timeframe of the information, including how far back the de-identified information goes in terms of dates of patient visits;
- the total number of individuals, or an approximation of the number of individuals, represented in the de-identified information; and
- the date or dates that the respondents or any one of the respondents transferred the de-identified information to the data purchaser.

[57] The respondents advised that the de-identified information may be accessed by the data purchaser on an ongoing basis, the information may concern patient visits from 2007 to 2021 and the number of individuals whose personal health information was used to generate the de-identified information depends on each "data retrieval", however the database available includes up to two million patient records. The respondents further advised that they do not have the precise date of the initial disclosure of the de-identified information, however noted that that the agreement was entered into with the data purchaser in March 2013.

[58] It is important to note that during this investigation the respondents took the step of amending the custodian's privacy policy. The amended privacy policy now informs individuals that their personal health information may be used for the purpose of de-identification and that the de-identified information may be sold to a third party for a number of purposes including for health related research.

The IPC's Finding

[59] Applying the modern approach to statutory interpretation set out above under paragraph 18, I will consider whether the privacy policy of the custodian complied with the requirements set out under 16(1)(a) of the *Act*, as informed by subsection 10(1) and the definition of "information practices" set out in section 2.

[60] Subsection 10(1) provides that a custodian "shall have in place information practices that comply with the requirements of this Act". If the definition of "information practices" cited at paragraph 51 above is broken down, it includes when and how personal health information is routinely used and modified, in addition to the purpose of each of these actions taken by the custodian.

[61] The term "routinely" is not defined under the *Act*. The Meriam Webster dictionary defines "routinely" as "a matter of regular occurrence".[9] The definition of "information practices" also refers to the terms "use" and "modify." The term "use" is defined in section 2 of the *Act* to mean "to view, handle or otherwise deal with the information" as set out above under paragraph 13 of this decision. The term "modify" is used in a number of provisions in the *Act* including 37(1)(f) and is not defined but, as was stated above in paragraph 39, the Oxford dictionary defines "modify" as "to change something slightly, especially in order to make it more suitable for a particular purpose".[10]

[62] Subsection 16(1)(a) of the *Act* requires a custodian, in a manner that is practical in the circumstances, to make available a written public statement that provides a general description of the custodian's information practices. The Meriam Webster dictionary defines "general" as "involving, applicable to, or affecting the whole" and "involving, relating to, or applicable to every member of a class, kind, or group".[11] The Oxford dictionary defines "general" as "affecting all or most people, places or things".[12]

[63] Based on the wording of subsection 16(1)(a), informed by subsection 10(1) and the definition of "information practices" at section 2 of the *Act*, it was not the intention of the Legislature to require custodians to describe every information practice in its

---

[9] Definition of "routinely", Merriam-Webster Online Dictionary: https://www.merriam-webster.com/dictionary/routinely.
[10] Definition of "modify", Oxford Learner's Dictionary: https://www.oxfordlearnersdictionaries.com/definition/english/modify.
[11] Definition of "general", Merriam-Webster Online Dictionary: https://www.merriam-webster.com/dictionary/general.
[12] Definition of "general", Oxford Learner's Dictionary: https://www.oxfordlearnersdictionaries.com/definition/english/general_1?q=general.

written public statement. However, applying the grammatical and ordinary meaning of subsection 16(1)(a), I find that a custodian must at least make available a written public statement that provides a "general" description of these information practices. A fair, large and liberal interpretation of the term "general" to information practices under subsection 16(1)(a) of the *Act* requires a custodian to describe its information practices in a general manner by providing notice of a routine or wide ranging practice that affects all, most or a substantial number of individuals or of a significant practice.

[64] Accordingly, I find that the custodian's description of its information practices must include the process of de-identifying personal health information which, for the reasons established above, involves the use of personal health information insofar as the information is being handled or dealt with, and the modification of personal health information insofar as the information is being changed or certain information is being removed in order to conceal the identity of the individual. The grammatical and ordinary meaning of subsection 16(1)(a), as informed by subsection 10(1) and the definition set out in section 2, further requires that the custodian describe the purpose of its de-identification process or action as part of its information practices.

[65] My interpretation of subsection 16(1)(a) is also consistent with the objects of the *Act*. As stated earlier in this decision, at its core, the objects or purposes of the *Act* are to protect the privacy of individuals in respect of their personal health information and the confidentiality of that information while facilitating the effective provision of health care, and to provide effective remedies for contraventions of the *Act*. Privacy and confidentiality are best protected by holding custodians accountable for the collection, use and disclosure of personal health information.

[66] If the transparency requirements set out in subsection 16(1)(a) of the *Act* are interpreted to mean that a custodian does not need to describe its regular, wide ranging or routine practice of de-identifying personal information which involves its use and modification, and the corresponding purposes, this would mean that custodians would likely not be held accountable for this use and modification of personal health information. For instance, if a custodian failed to de-identify the personal health information properly, an individual would not even be made aware of this practice so that they may inquire about it or make an informed decision on whether to provide their personal health information to the custodian or rather go to another custodian instead.

[67] The order making powers of the Commissioner under Part VI of the *Act*, titled "Administration and Enforcement" also specify that an order can be made directing any custodian whose activities the Commissioner reviewed "to change, cease or not commence an information practice specified by the Commissioner, if the Commissioner determines that the information practice contravenes this Act or its regulations" and "to implement an information practice specified by the Commissioner, if the Commissioner determines that the information practice is reasonably necessary in order to achieve compliance with this Act and its regulations". These remedies further support the meaning of the transparency requirements under subsection16(1)(a) of the *Act*, which would

permit an individual to be informed of the information practices and seek recourse by submitting a complaint to the IPC. Without being informed of a de-identification practice, no such recourse from the Commissioner can be sought, undermining one of the core objects of the *Act* at subsection 1(e).

[68] The respondents are correct in highlighting in their responses that there are no IPC decisions or orders issued by the IPC that have interpreted the application of the requirements under subsection 16(1)(a) with respect to the permitted use provision under subsection 37(1)(f). The respondents are also correct that IPC guidance has not touched upon the interpretation of subsection 16(1)(a) in this context. I have interpreted the meaning of subsection16(1)(a), informed by subsection 10(1) and the definition of "information practices" set out in section 2, in accordance with the modern approach to statutory interpretation as set out by the Supreme Court of Canada. Given that this issue has not come before the IPC for determination, I reject the respondents' submission that they are being held to a higher standard than that applied to other organizations. As stated above in this decision, and as per my delegated authority from the Commissioner, my role is to interpret the provisions of the *Act*, particularly when a fact scenario arises and/or a provision of the *Act* is engaged that has not yet been considered and applied by the IPC. With respect to the respondents' submission regarding the IPC's guidance documents, while they may help explain and simplify certain requirements under the *Act*, they do not purport to cover every factual circumstance, context and legal requirement that may apply under the *Act*.

[69] Finally, the table provided by the respondents highlighting that other custodians' privacy policies with the exception of one do not address de-identification of personal health information, does not assist the respondents in this investigation. As stated above in this decision, if other custodians are using personal health information in contravention of the *Act*, this does not assist me in determining whether the custodian has complied with its obligations under the *Act*.[13] The conduct or actions of any other person not named in this investigation is not before me in this matter.

[70] I find that the custodian in this investigation is required to include in its privacy policy the purpose of its de-identification practices which involve the use and modification of personal health information. I find that the use and modification of personal health information by the custodian and disclosing this data on an ongoing basis would meet the definition of a routine use and modification referred to in section 2 and therefore subsection 16(1)(a) requires that these actions and the purposes of these actions be described in the custodian's information practices.[14] I find the purpose of the use of personal health information by the custodian in this investigation is to modify the information in order to conceal the identity of the individual and the purpose of this modification is to sell the information to a third party. I further find that this routine and

[13] The table provided does not include any information on whether the listed custodians do in fact use personal health information, de-identify it and sell the information.
[14] See the definition of "information practices" under section 2 of *PHIPA* and subsection 10(1) of *PHIPA*.

wide-ranging practice must be included in the custodian's general description of its information practices in its written public statement under subsection 16(1)(a) of the *Act* as the practice was ongoing, the information concerned is from a significant time line (may date back to 2007) and that the volume of information and number of potentially affected individuals are significant (may include up to two million patient records). Individuals should be made aware of such practices of de-identification and their purposes, whether that may be research conducted by the custodian, sale or licensing of the de-identified information to a third party or for the purpose of retaining personal health information in a more secure manner.

[71] I find that the notice provided to individuals in the custodian's privacy policy that their personal health information may be used by the custodian for research, statistics and where permitted or required by law does not meet the above transparency requirements. However, given that the respondents have since taken the step of amending the custodian's privacy policy, I am satisfied that the custodian's privacy policy is now in compliance with the requirements under subsection 16(1)(a) of the *Act* insofar as it describes its practice of de-identifying personal health information and selling the information to a third party for a number of purposes, including for health-related research. This amendment addresses both the purpose of the use and modification of the personal health information.

Issue 4: Did the custodian take reasonable steps to protect the personal health information at issue in this matter?

[72] I now turn to the second question identified in paragraph 44 above, which is whether the custodian took reasonable steps in accordance with subsection 12(1) of the *Act* to protect the personal health information that was used and modified for the purpose of de-identification and sale.

[73] Subsection 12(1) of the *Act*, which is also found in Part II of the *Act*, requires that a custodian take "reasonable" steps to protect personal health information against theft, loss and unauthorized use and disclosure, among other things. Specifically, subsection 12(1) of the *Act* states:

> 12. (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modifications or disposal.

[74] In Order HO-010, the IPC stated that measures or safeguards must be reviewed from time to time to ensure that they continue to be "reasonable in the circumstances" in order to protect personal health information from theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized

copying, modification or disposal. In Order HO-010, the IPC further notes that as new technologies are developed, the "reasonable measures" standard in subsection 12(1) will evolve.

[75] I will now consider the measures taken by the custodian to meet its subsection 12(1) obligations.

De-Identification and Masking Strategy and Re-Identification Risk Assessment

[76] During this investigation, the respondents were asked to describe the steps taken by the custodian to comply with its subsection 12(1) obligations. The respondents stated that prior to disclosing information to the data purchaser, it was loaded onto a separate secure server and de-identification algorithms developed by a third party were applied to it. The respondents described the third party as having created an enterprise de-identification software which uses sophisticated de-identification techniques developed by industry-recognized privacy experts.

[77] In addition to creating and executing a de-identification and masking strategy, the third party produced an analysis of re-identification risks associated with the custodian's disclosure of the de-identified personal health information to the data purchaser. Two reports were produced by the third party, which were completed in 2014 and 2018 respectively (the 2014 report and the 2018 report). Both reports were provided to this office as part of its investigation.

[78] These reports set out the re-identification risk assessment performed by the third party, the considerations taken in deciding on an appropriate risk threshold, and the de-identification and masking that was performed by the software developed by the third party.

[79] As described in these risk analyses, the third party's process involved a number of steps. These included the development of a de-identification and masking strategy based on an analysis of the database of personal health information to be de-identified. Specifically, the third party identified which data elements (or 'fields') in the database could – alone or in combination with other information – uniquely identify an individual, and applied techniques such as masking (replacing the data with random data), suppression (replacing data with a 'null' value), or generalization (reducing the level of specificity of the data).

[80] The third party also determined context risk. This was based on questionnaires provided to the data purchaser that ask, among other things, how the recipient controls and safeguards any data it receives, what accountability measures it has in place, what contractual protections are in place with respect to this particular data, and the motive and capability of the recipient to re-identify the data. The third party stated in its reports that one of the assumptions made during its risk determination was that the answers to

those questionnaires were, to the best of the data purchaser's knowledge, reflective of its actual practices.

[81] An appropriate risk threshold (that is, the maximum acceptable likelihood that an individual could be re-identified) was also calculated, based on the sensitivity and potential injury to individuals in case of re-identification as well as past industry precedents for risk thresholds.

[82] Based on the above factors, the third-party made a calculation about the overall risk of re-identification and concluded in both the 2014 and 2018 reports that the risk was "very small" that the data could be used, alone or in combination with other reasonably available information, by the data purchaser to identify an individual. More specifically, it found that the overall risk of re-identification was below the acceptable risk threshold.

[83] The respondents state that the third party's de-identification and risk analysis strategies are "fully consistent with the IPC's guidelines", and that the third party used the same nine-step process set out in the IPC guidelines when developing the de-identification and masking strategy.

[84] The respondents have also stated that the de-identification techniques comply with the United States *Health Information Privacy and Accountability Act* (HIPAA)'s Expert Determination Method. The third party's 2018 report further stated that its process is also consistent with guidance from European regulators, and that it has been publicly documented and peer-reviewed.

Prohibition on use of identifiable information

[85] In addition to the third party's determination that the risk of re-identification was very small, the respondents submitted that the Sale Agreement prohibited any identifiable information being provided to the data purchaser and prohibited the data purchaser from using any identifiable information should it be inadvertently provided.

[86] The respondents state that the Sale Agreement provides that the data to be disclosed does not include any personal information as defined by applicable privacy legislation, or any data element that would permit the identification of any patient, and requires one of the named respondents to ensure that no such information is included.

[87] On the latter point, the respondents submitted that the Sale Agreement provides that in the event that any data or all or a portion of the data disclosed includes personal information or would permit the personal identification of a patient, the data purchaser is required to notify one of the named respondents and may not use the data except to de-identify it to the mutual satisfaction of both the named respondents and the data purchaser. The respondents confirmed that they have not received any such notification.

[88] In addition, the respondents note that the Sale Agreement further provides that

from time to time the data purchaser must have its data collection practices audited by an independent firm to ensure the data purchaser is not collecting patient-identifiable information unless collected with consent or in accordance with all applicable laws.

[89] The respondents also advised me that the data purchaser requires all employees, consultants and sub-contractors to sign a data confidentiality agreement which prohibits re-identification as well as "data linking"[15], and the data purchaser's clients are required to comply with standard operating procedures on data security and usage that specifically prohibit re-identification. Beyond this, the respondents state that data linking is not technically feasible, as there are no common patient identifiers in the data, and the respondents further confirmed that the data is not linked.

[90] During this investigation, this office raised the point that the Sale Agreement does not expressly forbid the data purchaser from linking data, nor does it require employees, consultants and sub-contractors of the data purchaser to sign data confidentiality agreements. While the respondents challenged the necessity of such a step (arguing that the nature of the de-identification applied to the database made linking data impossible, that the data purchaser was contractually prohibited from using any identifiable data, and that the data purchaser already required employees, contractors and sub-contractors to sign data confidentiality agreements), they nevertheless included these measures explicitly in the Amended Sale Agreement.

[91] It is also worth noting that in response to a question from this office, the respondents stated that any motivation the data purchaser may have to attempt to re-identify information was obviated as the purposes for which the data was provided would not be better served with the use of identifiable information and the de-identified information is designed to be useful in that (de-identified) format. The respondents also stated that the data purchaser has advised them that its leadership in the areas of privacy and information security are of paramount importance to itself and its entire client base. The respondents argue that the incalculable reputational risks which the data purchaser would be exposing itself to by attempting to re-identify the data would far outweigh any conceivable benefit from such re-identification.

Privacy and Security Controls

[92] During this investigation, the respondents were also asked whether a requirement to implement the privacy and security controls recommended in the IPC's *De-identification Guidelines*[16] was included in a data sharing agreement. The respondents advised that the primary means of evaluating the presence of such privacy and security controls was through the risk assessment undertaken by the third party, described prior. For each listed control, the respondents described the response provided by the data

[15] Data linking refers to combining records or information about a person from different sources; this can lead to the creation of information about an identifiable individual, even if one or both of the original records or information were not identifiable.

[16] IPC's "De-Identification Guidelines for Structured Data" (June 2016) at page 14.

purchaser during the risk assessment process, confirming that the data purchaser had established an internal policy which addressed the control in question (with the exception of a breach notification protocol between the data purchaser and the respondents, which was established through the Sale Agreement).

[93] However, the respondents also advised that privacy and security controls are now explicitly referenced in the Amended Sale Agreement. The Amended Sale Agreement requires the data purchaser to have in place a number of measures, including:

- Having all employees, consultants, and sub-contractors sign confidentiality contracts prohibiting data linking and/or re-identification;
- Only allowing authorized staff to access and use data on a "need-to-know" basis;
- Ensuring all employees, consultants, and sub-contractors working with the data receive adequate privacy and security training;
- Developing and maintaining data privacy, security, and usage standard operating procedures that specifically prohibit re-identification;
- Developing and maintaining strictly enforced retention, destruction and storage policies;
- Developing and maintaining role-based data access policies and processes, which are enforced and periodically audited;
- Maintaining records of all signed data-sharing agreements and confidentiality agreements, and making those available to the data custodian on request;
- Maintaining a proactive program for monitoring privacy, confidentiality and security polices and procedures, a mandatory and on-going training program for all individuals, and a breach protocol that is regularly updated and tested;
- Ensure that external and internal privacy reviews and audits are regularly conducted and that any identified gaps are mitigated.

[94] The above controls are largely equivalent to those set out in the responses provided to the third party by the data purchaser in the re-identification risk analyses. By virtue of the Amended Sale Agreement, the respondents have now ensured that these are included as explicit contractual requirements.

The IPC's Finding

[95] Based on the information provided above, and for the reasons below, I find that the custodian has taken reasonable steps in the circumstances, to ensure that the personal health information in its custody or control is protected against theft, loss and

unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modifications or disposal.

[96] In this circumstance, 'taking reasonable steps' includes determining whether appropriate measures were taken to ensure that the information sold was properly de-identified and that it is sufficiently unlikely that the information can be re-identified. These measures will generally include both the masking and de-identification strategy applied to the personal health information, and the safeguards established to protect against re-identification of the de-identified information.

[97] As described above, the respondents provided this office with copies of two re-identification risk analyses – from 2014 and 2018, respectively – which concluded that the risk of re-identification was very small. There is no information before me that suggests that these conclusions were incorrect.

[98] The respondents also took steps to prevent data linking and re-identification, and to ensure that appropriate privacy and security controls were in place. This includes a contractual prohibition on the use of any information that is determined to be identifiable, the unlikelihood of data linking given the nature of the de-identified information, confirmation from the data purchaser that the data is not linked, and consideration of the description of the privacy and security controls the data purchaser had in place as part of the risk analysis.

[99] In my view, although it would have been preferable for the prohibition against data linking and re-identification, and for the requirement to implement appropriate privacy controls to have been included as explicit contractual provisions in the original data sharing agreement, these have now been included in the Amended Sale Agreement.

[100] To be clear, there is no information before me that suggests that the information relied upon by the third party in its risk assessment was incorrect. Similarly, there is no information before me that suggests that data linking or re-identification occurred, or that appropriate privacy and security controls were not in place prior to the Amended Sale Agreement. Instead, I intend only to emphasize the importance of expressly including privacy and security controls and prohibitions against data linking and re-identification directly in a data sharing agreement.[17] Moreover, as will be described in the postscript of this decision, the *Act* has since been amended to prohibit any person from using or attempting to use information that has been de-identified to identify an individual, either alone or with other information. A related offence provision has also been introduced, punishable by fine or imprisonment, which will further serve to seriously dissuade any attempt to reidentify the data.

[101] Finally, in this particular context, I am satisfied that the de-identification and masking strategy used and the re-identification risk assessments (including the assertion

[17] IPC's "De-Identification Guidelines for Structured Data" (June 2016), privacy and security controls.

of the existence of appropriate privacy and security controls) were sufficiently robust.

Conclusion

[102] Again, taking all of the above into account, I am satisfied that the custodian has met its obligations under subsection 12(1) of the *Act* and taken reasonable steps to ensure the protection of the personal health information in the circumstances of this matter, including in light of the explicit privacy and security controls and the prohibition on data linking that have since been included in the Amended Sale Agreement.

Issue 5: Should this matter proceed to adjudication at the IPC, where a potential order may be issued*?*

[103] In the circumstances of this complaint, I found that the custodian's written public statement and information practices did not comply with the *Act*. However, during my investigation, the respondents took the step of amending the custodian's privacy policy to bring it into compliance with the requirements under subsection 16(1)(a) of the *Act*, with respect to their practice of de-identifying personal health information and selling the information to a third party.

[104] In addition to the above, I am satisfied that the custodian has complied with subsection 12(1) of the *Act*, in that reasonable steps have now been taken to ensure the protection of personal health information, particularly through the express privacy and security controls since added to the Amended Sale Agreement. Moreover, there is no information before me that suggests that the personal health information was not properly de-identified.

[105] In light of the steps taken by the respondents, I am satisfied that the issues in this matter have been resolved, and it is not necessary for this matter to proceed to the adjudication stage.

[106] Therefore, in accordance with my delegated authority under the *Act*, and for the reasons set out above, this review will be concluded without proceeding to the adjudication stage and without an order being issued.

Original Signed by: March 25, 2022

Lucy Costa
Manager of Investigations

POSTSCRIPT

The *Personal Health Information Protection Act, 2004* (the *Act*) was enacted more than 17 years ago. As technology evolves, the purposes for which health information custodians may collect, use and disclose personal health information may also change. Similarly, the types of safeguards that need to be employed to protect personal health information may also evolve with the technology being used and developed. As such changes take place, the *Act* may need to be amended from time to time to ensure the continued protection of privacy of individuals in respect of their personal health information and the confidentiality of that information and to provide effective remedies.

Since the commencement of this investigation, the *Act* was amended in 2019 to include limits on the use of de-identified information to identify an individual under section 11.2 of the *Act*. Section 11.2 of the *Act* provides:

> **Limits on use of de-identified information**
>
> 11.2 (1) Subject to subsection (2) and to any other exceptions that may be prescribed, no person shall use or attempt to use information that has been de-identified to identify an individual, either alone or with other information, unless this Act or another Act permits the information to be used to identify the individual.
>
> **Exceptions**
>
> (2) The limitation in subsection (1) does not prevent any of the following from using information that they de-identified, either alone or with other information, to identify an individual:
>
> 1. A health information custodian.
>
> 2. A prescribed entity mentioned in subsection 45 (1).
>
> 3. A prescribed person who compiles or maintains a registry of personal health information.
>
> 4. Any other prescribed person.

The offences provision under subsection 72(1) of the *Act* was also amended in 2019 to create a new offence in respect of any person who willfully contravenes section 11.2 of the *Act*.