Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 109

Complaint HI18-00035

A named individual

February 13, 2020

Summary: In this decision, the IPC concludes a review under the *Personal Health Information Protection Act, 2004* relating to allegations that a now former clinic employee improperly accessed personal health information of a number of patients of a clinic. The review was commenced pursuant to section 58(1) of the *Act*, which permits the IPC to conduct a review where there are reasonable grounds to believe that a person has contravened or is about to contravene the *Act*. This decision finds that the use and retention of personal health information by the former employee contravened section 17 of the *Act*. The respondent is ordered to not use or disclose any personal health information that she obtained as an agent of the clinic.

Statutes Considered: *Personal Health Information Protection Act, 2004,* sections 3(1), 4(1), 4(2), 6(1), 17, 37, 49, 58(1), 60(13), 61.

BACKGROUND:

[1] This review was commenced under section 58(1) of the *Personal Health Information Protection Act, 2004* (the *Act*), which permits the Information and Privacy Commissioner/Ontario (IPC or this office) to conduct a review of any matter where there are reasonable grounds to believe that a person has contravened or is about to contravene a provision of the *Act* or its regulations.

[2] In the spring of 2018, a patient (the Patient) of a family health clinic (the clinic) informed a physician at the clinic that she suspected a former clinic employee (the respondent) had accessed her personal health information for improper purposes. The respondent had left the clinic's employ in September 2017. In response, the clinic conducted audits of the respondent's accesses to the Patient's personal health information, held in the clinic's electronic medical records system (the EMR). The clinic found numerous

accesses to the Patient's personal health information that it concluded were not authorized under the *Act*. The clinic reported this as a privacy breach to the IPC.

[3] The clinic conducted additional audits of the EMR, finding numerous accesses by the respondent to the medical records of clinic staff and their family members. The clinic concluded that "there was no obvious work-related reason for such access[es]" and determined that these accesses were also unauthorized.

[4] In May 2018, clinic management met with the respondent and raised the issue of the accesses to the Patient's personal health information with her. The clinic reported that during that meeting the respondent claimed that all accesses were for work-related purposes.

[5] The clinic reported an additional incident to the IPC following this meeting, involving a phone call between a clinic employee and the respondent, which raised additional privacy concerns. According to the clinic, the respondent asked the employee to "do a favour for me, but it would be against the clinic", and stated that it was "about the [Patient]". The clinic reported that, on the call, the respondent asked the clinic employee to access the Patient's file.

[6] The clinic's response to the privacy issues raised by the above events was addressed in a separate file. This office opened this file with respect to the respondent. The clinic had identified a total of nine individuals, including the Patient, whose personal health information was accessed by the respondent without authorization, in the clinic's view. Eight of these nine individuals consented to having their personal health information included in my review. My review does not include the personal health information of the individual who did not consent.

[7] My review also did not address all allegations that the Patient raised with this office. Although the Patient made this office aware of additional allegations, she indicated that she did not wish to pursue them and this office respected her position. This review also does not address all of the remedies requested by the Patient or the respondent in their submissions. Some of these requested remedies are plainly outside the scope of this Review. To the extent that any of these requested remedies relate to personal health information that the respondent obtained as an agent of the clinic, they are addressed by my order issued at the end of this decision.

[8] During my review, I received written submissions from the respondent, the Patient and the clinic. The remaining affected parties were offered the opportunity to provide their own responses; they chose to have the clinic provide a response on their behalves.

[9] Through written submissions of the respondent, the IPC also became aware that the respondent had retained a great deal of personal health information about clinic patients after she ceased her employment at the clinic. After this was discovered, it also became an issue in my review.

[10] I have not identified the clinic or the respondent by name in this decision, as doing so may lead to identification of the Patient. This decision will be provided to the respondent, the Patient and the clinic with a confidential addendum which will not be made public by the IPC, and that identifies each by name.

DISCUSSION

The Issues

[11] The facts in this review raise concerns that the respondent may have used and/or retained personal health information in contravention of the *Act* in the following three circumstances:

1. The accesses to the clinic's EMR set out in the audit logs provided to the IPC by the clinic;

2. The telephone discussion between the respondent and a clinic employee after the end of the respondent's employment with the clinic, and

3. The retention of personal health information of clinic patients in the respondent's personal email accounts after the end of her employment with the clinic.

Statutory Provisions

[12] Broadly speaking, the *Act* regulates the activities of a group of persons described as "health information custodians" and their agents, with respect to personal health information. One of the purposes of the *Act* is to establish rules for the collection, use, and disclosure of personal health information by these persons, which protect the confidentiality of that information and the privacy of individuals while facilitating the effective provision of health care. One of the ways in which the *Act* achieves this purpose is by requiring that collections, uses and disclosures of personal health information occur with the consent of the individual to whom the information relates, unless the *Act* permits or requires this to be done without consent.[1]

[13] It is not in dispute and I find that the person who operates the clinic is a health information custodian. In particular, I find that they are a person who operates a group practice of health care practitioners pursuant to paragraph 1 of section 3(1) of the *Act*. It is also not in dispute that the clinic's EMR contains "personal health information" as defined in section 4, and that the clinic's audit records show accesses to that information.

[14] Under sections 17 and 37(2), a health information custodian that is permitted to use personal health information may, subject to other requirements, permit its agents to use that information as necessary to carry out their duties. Section 2 contains a definition of an "agent". While the nature of the respondent's duties is a matter of dispute between the respondent and the clinic, it is not in dispute that, during the period of her employment with the clinic, the respondent was an agent of the clinic within the meaning of the *Act*.

[15] Also relevant to this matter are the definitions of "use" and "disclose", set out in section 2:

> "disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian

[1] See s. 29 of the Act.

> or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;
>
> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means 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.[2]

[16] Section 17 of the *Act* addresses the circumstances in which an agent may use, disclose or retain personal health information, reading in part as follows:

> 17 (1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
>
> (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;
>
> (b) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and
>
> (c) the prescribed requirements, if any, are met.
>
> (1.1) A permission granted to an agent under subsection (1) may be subject to such conditions or restrictions as the health information custodian may impose.
>
> (2) Subject to any exception that may be prescribed, an agent of a health information custodian may collect, use, disclose, retain or dispose of personal health information only if,
>
> (a) the collection, use, disclosure, retention or disposal of the information, as the case may be,
>
> (i) is permitted by the custodian in accordance with subsection (1),
>
> (ii) is necessary for the purpose of carrying out his or her duties as agent of the custodian,
>
> (iii) is not contrary to this Act or another law, and
>
> (iv) complies with any conditions or restrictions that the custodian has imposed under subsection (1.1); and

[2] The definition of "use" was amended on June 3, 2016, but this legislative change has no impact on my decision. I have quoted from the current version.

(b) the prescribed requirements, if any, are met. [3]

[17] Section 6(1) of the *Act* provides that the provision of personal health information by a custodian to an agent of a custodian is a use and not a disclosure or collection.

1. The accesses to the clinic's EMR as set out in the audit logs provided to the IPC by the clinic

[18] As indicated above, this matter began with a report to this office by the clinic, alleging multiple unauthorized accesses by the respondent to the personal health information of the Patient. The clinic later made additional allegations of unauthorized accesses to the personal health information of other patients. I began my review by sending the respondent a Notice of Review, which included a summary of the allegations and the audit logs showing accesses (uses) that the clinic concluded were not authorized. I asked the respondent to confirm that she accessed the personal health information as indicated in the audits, whether the accesses were for work- related purposes, and invited her to respond to the clinic's findings. I also asked her if she has retained personal health information of any of these patients, in any format.

[19] The respondent provided a detailed response, which included commentary on the accesses listed in the audit logs, and a detailed description of her role at the clinic. The respondent's depiction of her role at the clinic differed significantly from the description provided by the clinic. She stated that her position was the Director of Prevention & Chronic Conditions, and described wide-ranging responsibilities, including training, querying the EMR system for matters for follow up, and addressing third party requests, in addition to her reception duties. She stated that her remote access was necessary to ensure that emergency hospital visits were being followed up, that fee for service doctors were sufficiently booked, and for data management, among other reasons.

[20] The respondent questioned the clinic's conclusion that the accesses highlighted in the audit logs were unauthorized. In a number of these entries, she questioned whether she had been the individual to access the information, stating that staff members' logins were known among staff and passwords were common to the logins. The respondent asserted that some of the family members of staff did work for the clinic, and could have used the respondent's account.

[21] The respondent provided possible reasons she may have made the accesses. For those accesses where she did not provide a specific reason for the access or confirm that she had made the access, the respondent stated that if she had accessed the personal health information, it would have been to fulfill her work responsibilities.

[22] With respect to a specific subset of the alleged unauthorized accesses, the respondent stated that she was out of the country at the time they occurred. She provided travel documents to support her position. The audit logs indicated that these accesses occurred from "Inside" the clinic.

---

[3] Section 17 of the Act was amended on June 3, 2016, and I have quoted from the current version. Since the facts about which I make findings in this decision all occurred following these amendments, it is unnecessary to have reference to the earlier provisions.

[23] The respondent denied retaining the personal health information of any of the patients identified in the audit logs. However, along with her representations, she provided a copy of email correspondence sent from the respondent's personal Gmail account to another staff member during the time she was employed at the clinic. Attached to this email were lists of clinic patients' names, email addresses, telephone numbers, and details of their prescription medications.[4] The respondent also provided the IPC with other emails from her personal email accounts containing the personal health information of clinic patients.

[24] After receiving the respondent's representations, I provided them (with some severances) to the clinic and the Patient with an Amended Notice of Review[5], and invited their response. The clinic maintained that the respondent's duties were largely administrative in nature, describing the respondent's role as follows:

> [The respondent's] depiction as a receptionist/secretary reflects most of what she did at the clinic. Basically, most of her day was spent handling incoming and outgoing calls, scheduling patients, taking care of any administrative request from the doctors, manning the front desk to register patients coming into the clinic, handling most 3rd party requests from lawyers and insurance companies (typically making copies of tests or clinic notes and mailing them), and sending e-mail for appointment reminders.
>
> Near the end of her employment she had been given the title of "Director, Chronic Conditions and Preventions" in anticipation of possibly using her to assist the lead physician …Because most of the other research assistants … would have had university degrees in science, many with MSc's, it would have been difficult for [the respondent] to work with them if it was known she was coming from a receptionist role.

[25] The clinic disagreed that the respondent's responsibilities required that she access personal health information to the extent reflected in the audit logs. The clinic stated that staff members had different usernames and different passwords. The exceptions were some position-specific accounts, such as front desk, telephone, and fax, which were accessed by whichever staff member was working that role. The clinic manager was the only staff member who knew the respondent's login credentials. The clinic elaborated on both why it found the accesses listed in the audit logs to be unauthorized, and why it believed that only the respondent made these accesses. Among other things, the clinic concluded that the remote accesses listed in the audit logs must have been made by the respondent, as other staff could be eliminated via an analysis of staff scheduling. The clinic noted that the respondent was the only support staff member to be provided with remote access to the EMR.

---

[4] After receiving the respondent's representations, I issued a determination pursuant to section 60(13) of the Act finding that, in order to carry out my review, it was reasonably necessary for me to inspect a record of, require evidence of, or inquire into the personal health information of the additional individuals included in the respondent's representations without their consent and that the public interest in carrying out the review justified dispensing with obtaining their consent in the circumstances.

[5] The Notice of Review was amended to include both the respondent's representations and the determination I issued pursuant to section 60(13) of the Act. The affected parties, other than the Patient, decided not to submit representations, instead opting to have the clinic submit representations on their behalves.

[26] The clinic did not dispute the respondent's evidence that she was outside the country during the time of certain accesses. The clinic acknowledged that the clinic manager logged on with the respondent's credentials while she was out of the country, stating that he did so in order to ensure that requests sent to the respondent were dealt with in her absence.[6]

Analysis

[27] The representations of the respondent and the clinic are hard to reconcile. As described above, they differ widely in their descriptions of the respondent's role while she worked at the clinic and her level of responsibility. Most importantly, the clinic maintains its position that the accesses shown on the audit logs (apart from those of the clinic manager) were unauthorized as they were not required to fulfill the respondent's work duties. The clinic provided over twenty pages of audit logs, identifying dozens of accesses to the personal health information of the eight affected patients. The clinic determined all of these to be made without authority under the *Act*.

[28] The respondent provided convincing explanations disproving some of the allegations of unauthorized accesses. In particular, I am satisfied that she was not responsible for the accesses that occurred while she was out of the country.

[29] While accepting the respondent's explanations for these specific allegations, I do not accept her explanation for others. I am referring specifically to three accesses to the Patient's personal health information on March 28, April 17 and April 29, 2017. These three accesses were the subject of detailed submissions from both the clinic and the respondent.

[30] First, the clinic noted that these accesses occurred from outside the clinic. The clinic also stated that the respondent was the only support staff member to be provided with remote access to the EMR. The respondent did not dispute these points. Second, while the respondent maintained that EMR passwords were shared and usernames were known amongst staff, she did not dispute the clinic's evidence that knowledge of her password would not in itself permit remote access. The respondent did not suggest that clinic staff ever used her credentials for remote access (the specific examples of other staff members using her credentials that she provided appear to have all occurred from inside the clinic). The respondent's own evidence is to the effect that she was granted remote access specifically to enable access while she was out of the country in 2015.

[31] Third, the clinic states that these remote accesses were linked to one IP address, which it concludes must be from the respondent's residence, and that it eliminated the possibility of other staff involvement by comparing these accesses with timesheets. None of these points, which were shared with the respondent, were refuted by her.

[32] Taking into account all of the above, I conclude that the respondent was responsible for the accesses to the Patient's personal health information on March 28, April 17 and April 29, 2017. The length of these accesses was about 15 minutes, 8 minutes and 12 minutes, respectively. In each case, the respondent accessed doctor's notes in the Patient's personal

---

[6] The representations sent during this review raise concerns about the clinic's practices for protecting personal health information, and whether it has complied with section 12(1) of the Act. The IPC will be opening another file to address these concerns, as they fall outside the scope of this review.

health information.

[33] Having concluded that the respondent was responsible for these three accesses, I will next determine whether they were authorized under the *Act*.

[34] As noted above, the clinic and the respondent disagree on the extent of her authority to deal with personal health information as an agent of the clinic. In explaining why she may have accessed the Patient's health record on the three occasions in question, the respondent described her role as follows:

> For instance the chart accesses from outside for [the Patient] on March 28, April 17 and April 29, 2017 were all under 15 minutes could be to check if the doctor's notes are up-to-date and if there is a need to book or modify follow-up appointment.
>
> …
>
> After closing clinic, if pending client are recollected, I would use remote access. It could be to check if the doctor's notes are up-to-date, test results and hospital reports are received in full and if there is a need to book or modify follow-up appointment. This was an implied expectation of my role.

[35] In response, the clinic states that this is:

> …a blatant falsehood. Nobody checks that doctor's notes are "up-to-date", there was/is no such function at this clinic, never has been. She was never taught to do so, nor expected to do so. When a doctor finishes a note (i.e. she selects "save & sign") at which point the colour of the chart in the day's schedule changes to green. Because of the change in colour it is easy to see which charts are completed and which are still incomplete and therefore, there is no need for anyone to access the chart and look at the notes "…to check if the doctor's notes are up-to-date…".
>
> Similarly, test results (bloodwork) and hospital reports are received electronically and are automatically attached to the patient's chart as well as being listed in the ordering physicians' inbox. There is no need for anyone to "check… if test results and hospital reports are received…". In fact, it is virtually impossible to check for them unless someone specifically identifies a patient and a test/report. Again, there was/is no such function at this clinic, never has been.
>
> …
>
> ***The important point, again, is that even if she were doing these useless activities, she should only have been accessing charts of patients who had an appointment (99% of tests are ordered during an appointment). [The respondent] has not explained her frequent accesses of charts, particularly that of [the Patient],*** **when** ***there was not*** **[sic]** ***test or appointment.***
>
> …

> Outside access, which [the respondent] admits, had only one IP address: [IP address removed]. I conclude that this was the IP address coming from her residence. ALL staff can be eliminated by comparing outside access with timesheets. To suggest that it was an IP address done by the access of another staff would require a conspiracy among staff that defies logic.
>
> …
>
> The three accesses of [the Patient's] chart are at a time when [the patient] did not have any appointment. Unlikely she would have been asked to contact her. Plus, there is no need to look at Doctor's notes. "…to check if the doctor's notes are up-to-date…" is a fabrication…
>
> [Emphasis in original]

[36] In the above, the clinic provided a specific and clear rebuttal of the respondent's explanation for these remote accesses, with reference to the functionality of the EMR and the fact that the Patient did not have appointments (which would have made the respondent's other explanations more likely). This submission was provided to the respondent who did not specifically address it.

[37] In assessing the evidence regarding these accesses, I have also considered the facts of the telephone conversation that occurred about one month after the meeting at which the clinic confronted the respondent with the allegations of unauthorized access.

[38] The clinic states that the respondent sent a text message to a clinic employee asking that the clinic employee call her. According to the clinic, when the clinic employee telephoned the respondent, the respondent asked her to "do a favour for me, but it would be against the clinic", and stated that it was "about the [Patient]". The clinic reported that the respondent asked the clinic employee to access the Patient's file during that call. The clinic states that no further discussion of the Patient took place on this call as the clinic employee advised the respondent to speak to the clinic manager. The employee reported this conversation to the clinic manager.

[39] The clinic indicated that the clinic employee was not aware of the allegations against the respondent with respect to the Patient's personal health information.

[40] The respondent briefly addressed this phone call in her representations. She acknowledges that the call occurred and did not deny the clinic's account of the conversation. She asserts, however, that "no patient information was shared during the call" and that the purpose of the call was for "networking and employment opportunities."

[41] I accept the clinic's evidence as to the contents of this phone call. In my view, these facts are relevant to assessing whether the remote accesses made by the respondent to the Patient's personal health information were authorized. At the very least, they suggest a purpose for the respondent's accesses to the Patient's personal health information beyond the ones she gave in her representations. I infer that the respondent had a particular, non-work related, interest in this specific Patient.

[42] Based on all of the above, I find that the respondent's accesses to the Patient's

personal health information were not for the purposes of providing or assisting in the provision of health care to her. They were also not permitted by the clinic. On balance, the evidence does not support a conclusion that these accesses were authorized under the *Act*, for health care or another permitted purpose, with or without the Patient's consent. I find that these remote accesses to the Patient's personal health information on March 28, April 17 and April 29, 2017 were an unauthorized use of personal health information by the respondent.

2. The telephone discussion between the respondent and a clinic employee after the end of the respondent's employment with the clinic

[43] Above, I examined the telephone call between the respondent and the clinic employee that occurred after the end of the respondent's employment at the clinic. I found that, on this call, the respondent asked the clinic employee to "do a favour for me, but it would be against the clinic", stated that it was "about the [patient]" and further asked the clinic employee to access the Patient's file. I determined that this call was relevant to my analysis of whether the remote accesses to the Patient's personal health information were unauthorized. Arguably, the discussion during this phone call was itself a use of personal health information, without authority under the *Act*.

[44] However, it is not necessary for me to make a specific finding on this issue as it would not affect the orders I have decided are appropriate in this matter.

3. The retention of personal health information in the respondent's personal email accounts after the end of her employment with the clinic

[45] The clinic did not identify this as an issue when it notified the IPC of this matter. As described above, the information provided by the respondent herself, during the course of this review, provided evidence of a potential additional breach of the *Act*. In particular, the respondent indicated that she had retained multiple patients' personal health information after the end of her employment with the clinic.

[46] Since this was not included in the Notice of Review initially sent to the respondent, I amended the Notice of Review and invited the clinic, the Patient, and the respondent to make additional representations on the issues raised by the respondent's apparent unauthorized retention of patient information.

[47] The respondent states in her representations that her responsibilities included distributing patient medication list emails to each doctor, and that she did so from her personal email because the clinic had not created office email addresses for document sharing. This is consistent with the clinic's representations, in which the clinic stated that it was "aware that [the respondent] was using her personal e-mail to send [the medication lists]".

[48] Regarding the retention of the personal health information, the clinic stated that the respondent's employment and confidentiality agreements did not explicitly state that personal health information should not be held after employment ceases, but stated that to conclude otherwise would be "stretching" these same agreements. The clinic provided excerpts from an agreement signed by the respondent, in which the respondent acknowledged that her obligation of patient confidentiality continues after her termination

of employment, and that all records of confidential information should be surrendered at the termination of her employment.

[49] After I sought the respondent's representations on a potential order resulting from this review, in relation to her retention of personal health information obtained as an agent of the clinic, the respondent provided me with a signed affidavit in which she stated:

> I have already properly deleted and destroyed the records of patient personal health information from the [clinic] that I have in possession [sic] and all copies thereof.
>
> I am no longer in possession of any patient personal health information from the [clinic].

Analysis

[50] It is not in dispute that the information contained in the medication lists attached to the respondent's email is personal health information. I note that other information about patients contained in emails provided by the respondent to the IPC also plainly includes personal health information.

[51] There is no dispute, and I find, that the respondent retained personal health information relating to patients of the clinic after her employment at the clinic ended.[7] The issue at hand is whether the respondent's retention of this personal health information was authorized under the *Act*.

[52] Neither the clinic nor the respondent have taken the position that the respondent's retention of personal health information was authorized. The clinic stated that any continued retention of personal health information contained in emails was not explicitly addressed in its written agreements with the employee, but described a former employee having any right to possess such information after termination as "troubling". The respondent, in her representations, sets out the reasons why she emailed the personal health information from her personal email accounts during her employment, but is silent on whether her continued retention was authorized under the *Act*. As noted above, the respondent subsequently provided an affidavit attesting to her destruction of these records.

[53] While this affidavit addresses the destruction of the records, it does not negate the fact that the respondent retained them well beyond the time her role as an agent of the clinic ended. As discussed below, it also does not address the personal health information the respondent may have knowledge of through her role as an agent of the clinic, but not have in a record.

[54] As noted above, section 17(2) of the *Act* states that an agent of a health information

---

[7] The clinic has not alleged that the respondent's sending of personal health information from her personal email during the course of her employment was contrary to the Act. Whether that use of personal health information by the respondent was authorized under the Act is not at issue in my review. However, as noted above, this raises further concerns about the steps taken by the clinic to protect personal health information in its custody or control that will be addressed in a separate file, to be opened by the IPC with respect to the clinic.

custodian may only retain personal health information if certain conditions are met. One of those conditions, as set out in section 17(2)(a)(ii) of the *Act*, is if the retention of the information "is necessary for the purposes of carrying out his or her duties as agent of the custodian."

[55] The respondent was an agent of the clinic when she obtained these records of personal health information, and no one has disputed that this provision continued to apply to the respondent after her departure. In my view, the obligations under section 17(2) must continue after an agent ceases having a role with a custodian (with respect to personal health information obtained while an agent). Otherwise, an agent could simply quit and be free, under the *Act*, to use, disclose or retain personal health information they obtained while an agent.

[56] In this case, the respondent retained personal health information, without having any duties that would necessitate the retention of that information. As such, her retention of these records for over two years, from the time when her employment at the clinic ended to the time the records were destroyed, was a contravention of section 17 of the *Act*.

[57] Before concluding, I should also note that the respondent has suggested at various points in her submissions that the clinic reported this case to the IPC in order to harass her for filing an employment standards claim against the clinic. This allegation of harassment in relation to this IPC file appears to be nothing more than a bald claim. There is no evidence indicating that the clinic's intention was to harass the respondent with this report to the IPC. The clear evidence is that this matter came to light as a result of information provided to the clinic by the Patient. I reject this allegation by the respondent.

What order, if any, should be issued?

[58] Section 61(1) of the *Act* permits the IPC to issue the following relevant orders: Powers of Commissioner

> 61 (1) After conducting a review under section 57 or 58, the Commissioner may,
>
> > (c) make an order directing any person whose activities the Commissioner reviewed to perform a duty imposed by this Act or its regulations;
> >
> > (d) make an order directing any person whose activities the Commissioner reviewed to cease collecting, using or disclosing personal health information if the Commissioner determines that the person is collecting, using or disclosing the information, as the case may be, or is about to do so in contravention of this Act, its regulations or an agreement entered into under this Act;
> >
> > (e) make an order directing any person whose activities the Commissioner reviewed to dispose of records of personal health information that the Commissioner determines the person collected, used or disclosed in contravention of this Act, its regulations or an agreement entered into under this Act but only if the disposal of the

> records is not reasonably expected to adversely affect the provision of health care to an individual;

[59] Above, I have found that the respondent used personal health information of the Patient in contravention of the *Act* and retained personal health information of many clinic patients in contravention of the *Act*.

[60] The respondent has provided an affidavit indicating that she has deleted and destroyed the records of clinic patients that she previously retained. However, this affidavit does not address other potential uses or disclosures of personal health information that the respondent has knowledge of through her role at the clinic. I have found that the respondent did, in fact, use the Patient's personal health information in contravention of the *Act*.

[61] I have also found, above, that section 17 of the *Act* applies to the respondent and, among other things, restricts her from using, disclosing or retaining personal health information that she obtained as an agent of the clinic, even after she left the clinic.

[62] In light of the contraventions that have occurred and my findings above, I believe it is appropriate to order that the respondent not use or disclose any personal health information that she obtained, or has knowledge of, through her role as an agent of the clinic including, but not limited to, the Patient's personal health information. This order does not restrict the respondent from providing personal health information where required by law (for example, required by a valid court order). Further, this order does not deprive the respondent of other statutory disclosures that she could make as an agent under section 7 of O. Reg. 329/04 under the *Act*.

[63] Effectively, this order obliges the respondent to comply with pre-existing obligations under the *Act.* I have found that she has not always previously complied with these obligations. As such, this order is issued under s. 61(1)(c) of the *Act*.

ORDER:

For the foregoing reasons and pursuant to section 61(1) of the *Act,* I order that:

1. The respondent shall not use or disclose any personal health information, whether in oral or recorded form, in whatever medium this may be maintained, that she obtained and/or has knowledge of through her role as an agent of the clinic, including the personal health information of the Patient.

2. Order provision 1 does not restrict uses or disclosures of personal health information by the respondent as required by law or pursuant to section 7 of O. Reg. 329/04.

Original signed by: February 13, 2020

Sherry Liang
Assistant Commissioner