Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 51

Complaint HI15-61

A prescribed person

September 12, 2017

Summary: This investigation was opened under the *Personal Health Information Protection Act* (*PHIPA*) as a result of a privacy breach report which was received by the Office of the Information and Privacy Commissioner/Ontario (the IPC or this Office) with respect to an unauthorized disclosure of personal health information by a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care (the Registry). The IPC finds that a review of this matter is not warranted.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 4(1), 4(2), 58(1), and 39(1)(c); Ontario Regulation 329/04 section 13.

Decisions considered: *PHIPA* Order HO-011

INTRODUCTION:

The Registry disclosed to an individual (the complainant) medical test results relating to another individual with the same first name, last name, sex, and date of birth as the complainant. The complainant had not undergone the test for which she received results, but received test results relating to the individual who had undergone this test (the patient).

BACKGROUND:

[1] On April 28, 2015, the IPC received a complaint from the complainant regarding a letter she received from the Registry. This letter contained the complainant's name, address and details regarding the results of a particular medical test that appeared to relate to the complainant. The complainant informed the IPC that, although it was her name and address on the letter, she had not taken this particular test and, as such, the test results did not relate to her.

[2] Before complaining to the IPC, the complainant had contacted the Registry with her concerns and was dissatisfied with its response. When she advised the Registry that she had received test results that did not relate to her, she was told the Registry would look into it. The Registry's Laboratory Liaison followed up directly with the laboratory who had submitted the test results. The laboratory confirmed that the information included on the requisition forms matched the reported screening results and that no error had occurred. The laboratory then contacted the physician who had signed the requisitions in order to determine whether a labelling error had occurred at the physician's office. The physician advised the laboratory that a labelling error had not occurred and maintained that the test results belonged to the individual whose name appeared on the requisitions.

[3] The Registry then contacted the complainant and suggested she speak to her healthcare provider about the incident as the laboratory records indicated that a test had been completed in her name. The Registry provided her with the telephone number of the physician that had ordered the test. The complainant (who knew she did not have this test done) followed up with the office of the physician who ordered the test (who was not her physician) and was able to confirm that another individual with her same name was a patient of the physician. The complainant then relayed this information to the Registry.

[4] After receiving this information from the complainant, the Registry was advised by the laboratory that the physician's office had contacted the laboratory again and had confirmed that a labelling error had, in fact, occurred. As a result of this confirmation, the laboratory cancelled the test result and had the result removed from the database. In turn, the test result was removed from the complainant's profile on the Registry and placed in an "Unknown Person" profile. The Registry then contacted the complainant and advised her that a labelling error had been made by the physician, and that the test result had been removed from her profile.

[5] The complainant was dissatisfied with the explanation provided to her by the Registry and continued to have concerns with respect to how this error had occurred. As a result, the complainant filed a complaint with the IPC and the matter was assigned to an Analyst.

[6] In addition to the complaint received by the IPC from the complainant, on October 7, 2015 the Registry reported this matter to the IPC as a breach of *PHIPA*. As the privacy breach apparently related to another individual's personal health information

that was mistakenly sent to the complainant, the matter was then opened as a Commissioner initiated file and was assigned to the Investigation Stage of the IPC's *PHIPA* processes. The complainant was advised of this and understood that this matter would be investigated by the IPC. The complainant agreed that her complaint could be closed but requested that she be advised of the outcome.

[7] As part of my investigation I requested and received written representations from the Registry with respect to this matter. I also contacted and received information from the laboratory and the physician who signed the requisitions. The information I obtained is described below.

The Laboratory

[8] The laboratory explained that upon being made aware by the Registry of the complainant's concerns, it contacted the physician and was told that the physician did, in fact, take a sample and ordered it to be tested November 28, 2014. Subsequent to this conversation, the physician's office advised the laboratory that the test may have been mistakenly ordered as a result of a labeling error on their part.

[9] Given the discrepancies in the information being provided, I contacted the laboratory and requested a copy of the requisitions related to this matter. The laboratory responded and indicated that two requisitions were received from the physician on or about November 28, 2014. One was a standard requisition with a sample and the other was a requisition for a particular test. Both requisitions included the name, date of birth and gender of the complainant, however the address and phone number differed from that of the complainant. The requisitions also indicated that (unlike the complainant) the patient was not insured under the Ontario Health Insurance Plan (OHIP). The Laboratory advised that both requisitions were processed and sent electronically to a database which the Registry has access to and uses for, among other things, contacting patients with test results.

The Physician

[10] During this investigation the Registry advised this office that a labelling error had occurred on the part of the physician who completed the requisitions. After reviewing the requisitions, I contacted the office of the physician and was provided with written confirmation that a patient with the same name and date of birth as the complainant was indeed a patient of the physician. I also received written confirmation that the address written on the requisitions matched the patient's address in the physician's records. Despite the information originally provided to the IPC, no labelling error occurred.

The Registry

[11] The address on the letter that was sent to the complainant did not match the address that was provided to the Registry by the laboratory. I asked the Registry how

the address of the complainant became attached to the test results of the patient. The Registry has explained, as summarized below, why the address was changed and acknowledged that it was an error.

[12] The Registry explained that it uses an information management/information technology solution (Solution) that integrates and links disparate data sets from a variety of data sources, such as the Ministry of Health and Long-Term Care's Registered Persons Database and other laboratory data, to create screening records for Ontarians. According to the information provided to this office, the Registry uses a linkage logic that has been in place since 2009. The Registry advised that this data linkage was reviewed and approved in accordance with its Data Linkage Policy.

[13] As of January 30, 2017, the Registry maintained the personal health information of approximately 8.9 million "Master Person profiles" of eligible Ontarians in the Solution. A Master Person profile is a record that identifies a patient by the following data elements: Health Insurance Number (if available), First Name, Middle Name (if available), Surname, Date of Birth and Gender. The same person may have more than one Master Person profile in the Solution.[1]

[14] In this case, the linkage rules used by the Registry system incorrectly identified the complainant as the patient, based on the fact that the test results for the patient (the individual who had the test performed) and the existing patient profile for the complainant (who did not have the test performed) in the Solution had the same values for the fields, surname, first name, date of birth and gender. Since an Ontario health number was not provided with the test results, the Solution only used the match criteria of surname, first name, date of birth and gender. The Registry explained that, where an Ontario health number is not provided, the Solution will only link to a master person profile where the data elements only match to one such profile.

[15] The test results provided to the Registry contained address information for the true patient, and this address did not match the address of the complainant. The Registry advised that it does not use the address field as part of its linkage rules because the addresses contained in the requisitions "… are not used to update client's addresses for the purpose of mailing correspondence since the data is considered to be of poor quality".

[16] The Registry confirmed that the fact that the patient was uninsured under OHIP (whereas the complainant was insured) would not trigger a flag that would require further investigation by the Registry into whether a correct match had occurred. It also confirmed that four data elements must match before the Registry's system considers two records to relate to the same person.

[1]The Registry advised that this would occur, for example, where two test results are received for the same person and on one test result the date of birth contained a typo. This would result in the creation of two Master Person profiles.

[17] The Registry also provided detailed representations regarding the frequency with which test results were incorrectly linked to existing patient profiles, which are discussed in more detail below.

[18] The Registry advised that, on the same day the complainant called, it commenced an investigation into this matter and ultimately reported this matter to the IPC as a self reported breach. The Registry notified the laboratory of this complaint and also later provided a notification letter to the physician who prepared requisitions in question. The Registry requested that the physician provide that letter to the patient. To date the patient has not contacted the IPC in regards to this matter.

[19] With respect to containment, the Registry advised that it took immediate steps to ensure that further disclosure of the patient's test result did not occur by removing the screening result from the complainant's Master Person profile and transferring it to an Unknown Person profile. The Registry advised that once a result is attributed to an Unknown Person profile, it is not disclosed until it can be successfully linked to an existing single Master Person profile.

[20] In this decision I find that an unauthorized disclosure of personal health information by the Registry occurred. I also find that a review is not warranted under *PHIPA*.

ISSUES:

1. Did the letter at issue in this matter contain personal health information and was it disclosed in accordance with *PHIPA*?

2. Is a review warranted under *PHIPA*?

RESULTS OF THE INVESTIGATION:

Issue 1: Did the letter at issue in this matter contain personal health information and was it disclosed in accordance with *PHIPA*?

[21] Section 4(1) of *PHIPA*, states, in part:

> In this Act,
>
> "personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,

> a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
>
> b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
>
> …

[22] Section 4(2) of *PHIPA* provides:

> In this section,
>
> "identifying information" 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.

Section 2 of *PHIPA* defines "disclose" as follows:

> "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 or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;

[23] The information contained in the letter included a name, address and details regarding the results of a particular medical test. The Registry has acknowledged the letter contained personal health information. There is no dispute, and I find, that the information at issue in the letter is personal health information within the meaning of *PHIPA*. There is further no dispute, and I find, that this personal health information was disclosed by the Registry, as it was mailed to the complainant.

[24] The Registry has confirmed that this disclosure of personal health information was not authorized by *PHIPA*. The Registry stated the following:

> The disclosure was not authorized by PHIPA, [the Registry] has many practices and procedures in place to prevent unauthorized disclosures of PHI, including [the Registry] Data Linkage Policy. [The Registry] acted in accordance with the Data Linkage Policy. In other words, this situation was not caused by a failure of [the Registry] to comply with its practices and procedures but instead was a function of the unique circumstances of this case.

[25] With respect to the disclosure, the Registry has confirmed that the recipient of

the letter was not the patient to whom the test results related. Simply put, the Registry mailed one individual's personal health information to the wrong individual with the same first name, last name, and date of birth. While the Registry notes that it acted in accordance with its Data Linkage Policy, I do not take it to be asserting that compliance with this policy means that disclosure, in error, of one individual's personal health information to another individual is authorized by *PHIPA*. Rather, I take the Registry to simply be noting that it complied with the letter of its data linkage policy, and that compliance with this policy, on the facts of this case, resulted in this unauthorized disclosure.

[26] No party disputes, and I find, that this disclosure was unauthorized by *PHIPA*.

[27] Having found that this disclosure was unauthorized, I will now consider whether a review of this matter is warranted under *PHIPA.*

Issue 2: Is a review warranted under *PHIPA*?

[28] In this investigation, my role is to consider whether the Registry's practices and procedures continue to protect the privacy of individuals whose personal health information it receives, and continue to maintain the confidentiality of that information. In particular, I have considered whether the Registry's practices and procedures require steps that are reasonable in the circumstances to ensure that personal health information in its custody or control is protected against unauthorized disclosure. Ultimately, after considering the above, I must decide whether a review of this matter is warranted under *PHIPA.*

IPC's Authority with Respect to the Prescribed Registry

[29] Section 39(1(c) of *PHIPA* provides:

> 39 (1) Subject to the requirements and restrictions, if any, that are prescribed, a health information custodian may disclose personal health information about an individual,
>
> …
>
> (c) to a prescribed person who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances;

[30] There is no dispute, and I find, that the Registry is a prescribed person for the purposes of section 39(1)(c) as set out in section 13(1) of Regulation 329/04.

[31] Section 13 of Ontario Regulation 329/04 prescribes the persons who compile or maintain a registry for the purposes of section 39(1)(c) and addresses the obligation on

such person to have their practices and procedures approved by the IPC every three years:

> 13. (2) A person who is a prescribed person for the purposes of clause 39 (1) (c) of the Act shall put into place practices and procedures,
>
> > (a) that are for the purpose of protecting the privacy of the individuals whose personal health information it receives and for maintaining the confidentiality of the information; and
> >
> > (b) that are approved by the Commissioner every three years.
>
> (3) A person that is a prescribed person for the purposes of clause 39 (1) (c) of the Act shall make publicly available a plain language description of the functions of the registry compiled or maintained by the person, including a summary of the practices and procedures described in subsection (2).
>
> (4) A person that is a prescribed person for the purposes of clause 39 (1) (c) of the Act may use personal health information as if it were a health information custodian for the purposes of clause 37 (1) (j) or subsection 37 (3) of the Act.
>
> (5) A person that is a prescribed person for the purposes of clause 39 (1) (c) of the Act may disclose personal health information as if it were a health information custodian for the purposes of sections 44, 45 and 47 of the Act.

[32] In Order HO-011 former Commissioner Ann Cavoukian addressed this office's authority to review the practices and procedures put in place by a registry outside of the process for reviewing those practices and procedures every three years and stated:

> As a prescribed person, the practices and procedures put in place by CCO for the purpose of protecting the privacy of the individuals whose personal health information it receives and maintaining the confidentiality of the personal health information are subject to approval by my office on a triennial basis. If approval is granted, and assuming that all other requirements in the Act and the Regulation are met, CCO has the authority to collect personal health information from health information custodians and to use and disclose this personal health information for the purposes of facilitating or improving the provision of health care, and for other purposes permitted by the Act and the Regulation, without the consent of the individuals to whom the personal health information relates. Correspondingly, section 39(1)(c) of the Act gives health information custodians the authority to disclose personal health

> information to CCO for the purposes of facilitating or improving the provision of health care.
>
> The requirement that CCO put in place practices and procedures for the purpose of protecting the privacy of the individuals whose personal health information it receives, and for maintaining the confidentiality of that personal health information ("practices and procedures"), and that these practices and procedures be reviewed and approved by my office every three years, is set out in section 13(2) of the Regulation. A further requirement that CCO make a plain language summary of its practices and procedures publicly available is set out in section 13(3) of the Regulation.
>
> …
>
> While a prescribed person or entity may put in place new or revised practices and procedures between triennial reviews, my office retains the authority to review new or revised practices and procedures pursuant to Part VI of the Act, if there are reasonable grounds to believe that they may contravene section 13 of the Regulation. Further, for the reasons set out above, including evolving privacy standards and best practices, the emergence of new privacy risks and the development of new technologies, my office also retains the authority under Part VI of the Act to review the practices and procedures put in place by a prescribed person or entity that were previously reviewed and approved by my office under section 13 of the Regulation, to ensure that these practices and procedures continue to protect the privacy of individuals whose personal health information it receives, and continue to maintain the confidentiality of that information.[2]

[33] I accept and adopt the approach taken in Order HO-011 with respect to the IPC's authority to review the Registry under Part VI of *PHIPA*.

Compliance with the Manual

[34] This office's expectations of prescribed entities under section 45 of *PHIPA* and prescribed persons (Registries) under section 39(1)(c) of *PHIPA* are set out in the *Manual for the Review and Approval of Prescribed Persons And Prescribed Entities* (the *Manual*) made available by the IPC.[3] The *Manual* is the core document that describes the practices and procedures that this office expects prescribed persons and prescribed

---

[2] Order HO-011, pp. 4, 22-23 – Online: http://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/135133/index.do

[3] Online: https://www.ipc.on.ca/wp-content/uploads/2016/08/MANUAL-FOR-THE-REVIEW-AND-APPROVAL-OF-PRESCRIBED-PERSONS-AND-PRESCRIBED-ENTITIES.pdf

entities will have in place.[4]

[35] Among other things, the *Manual* requires that, at a minimum, prescribed persons and prescribed entities develop and implement an overarching information security policy and that this policy "must require that steps be taken that are reasonable in the circumstances to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that the records of personal health information are protected against unauthorized copying, modification or disposal."[5] This mirrors the obligation imposed by section 12(1) of *PHIPA* on health information custodians, which 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, modification or disposal.

[36] Similarly, the *Manual* requires that prescribed entities and prescribed persons develop an overarching privacy policy that ensures that each disclosure identified in the privacy policy is consistent with the disclosures of personal health information permitted by *PHIPA* and its regulation.[6] As noted above, there is no dispute that this particular disclosure was unauthorized by *PHIPA.*

[37] The *Manual* further requires that prescribed entities and prescribed persons develop and implement policies and procedures with respect to privacy impact assessments, and recommends that privacy impact assessment be conducted "on existing and proposed data holdings involving personal health information and whenever a new or a change to an existing information system, technology or program involving personal health information is contemplated."[7]

[38] In this case, the complainant was linked to the patient because they had the same first name, last name, date of birth and sex, and because no health card number was provided for the patient. According to the Registry, 0.47% of master person profiles on the Solution will have the same first name, surname, date of birth, and sex as one or more other master person profiles. When the absence of an Ontario health number is considered, only 0.15% of master person profiles will have the same first name, surname and date of birth and sex.

[39] As of December 31, 2016, the Registry had mailed approximately 23.9 million

---

[4] While the IPC, where appropriate and as set out in the *Manual*, makes case-by-case exceptions to compliance with the provisions of the *Manual*, no such exceptions are relevant here.
[5] *Manual*, p. 75
[6] *Manual*, pp. 15, 17
[7] *Manual*, p. 62

correspondence letters that utilized this linkage logic. The Registry processed over two million screening tests per year in the years 2013, 2014 and 2015 and in each year processed over fifty thousand screening test results where there was no Ontario health number. In each of those years, the Registry linked over two million screening test results to an existing patient profile, and over thirty thousand of those screening test results in each year did not contain an Ontario health number. This incident is the only one known to the Registry in which a test notification was linked to the wrong patient profile.

[40] In its representations submitted as part of this investigation, the Registry submitted:

> The safeguards and practices utilized by [the Registry] are intended to mitigate the privacy risk that is inherent in data linkage practices. The linkage logic used in [the information management/information technology solution] was designed with privacy principles in mind. [The Registry]'s linkage logic was evaluated in PIAs and where risks were identified, mitigation strategies were implemented. The effectiveness of the linkage practices has been monitored over time. Since the introduction of the linkage logic in 2009, this is the first time, to [the Registry]'s knowledge, that an automatic linkage such as the one giving rise to the complaint has occurred. This is despite the very high volume of test results sent out annually by [the Registry] for its … screening programs.
>
> [The Registry] is of the view that its practices and procedures related to the protection of the privacy of individuals whose PHI has been entrusted to it have been reasonable in the circumstances. In addition, in light of this incident, and in accordance with [the Registry]'s ongoing practice to regularly review safeguards and practices to ensure they continue to be effective and reasonable, [the Registry] has undertaken an assessment of its linkage logic practices and is evaluating whether there are opportunities for improvement. At the completion of this assessment, there will be a recommendation made to [the Registry] management as to whether any changes are necessary. We will postpone making such a recommendation until we hear from the IPC in connection with this matter.

[41] The Registry provided this office with copies of a number of policies and other materials relevant to this matter. The Registry also provided this office with two privacy impact assessments relating to this screening program, both of which identify the risk that information will be linked incorrectly and thereby cause a privacy breach. Among other things, these privacy impact assessments recommend a mitigation strategy of monitoring such breaches to identify patterns or trends that can be rectified by changing data linking rules. The Registry indicates that it has monitored the effectiveness of its linkage practices over time.

[42] In this case, this privacy breach occurred because the Registry incorrectly linked the personal health information of the patient to the profile of the complainant. This error occurred because the patient and the complainant have the same first name, last name, sex, and date of birth, and because the patient did not have an Ontario health number. It would appear that this type of incorrect linkage has been very rare. I note that, of the over thirty thousand test results that did not contain an Ontario health number and that were linked to an existing patient profile in each of 2013, 2014 and 2015, this is the only known instance where an incorrect linkage occurred. The Registry indicates that it identified the risk of such an incorrect linkage and took steps to mitigate this risk by monitoring the effectiveness of its linkage logic over time. Based on the information before me, and in light of the fact this type of breach is only known to have occurred once, I conclude that a review is not warranted under *PHIPA.*

[43] This is not to say that the Registry cannot improve upon its linkage rules to ensure that a privacy breach resulting from an incorrect data linkage does not happen again. For example, where individuals have the same first name, last name, date of birth and sex, but there is no Ontario health number provided, the IPC would urge the Registry to consider whether there are other data fields or methods that could be utilized to ensure that such an incorrect linkage does not occur again. Of course, the Registry is urged to continue to monitor the effectiveness of its data linkage practices to ensure they continue to comply with *PHIPA* and the *Manual*. Should the Registry's data linkage practices lead to further incorrect linkages, this may be addressed by the IPC in the future, including as part of the IPC's three-year review of the Registry's practices and procedures.

NO REVIEW:

Section 58(1) of *PHIPA* states the following:

> Commissioner's self-initiated review
>
> **58** (1) The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention

For the foregoing reasons, no review of this matter will be conducted under PART VI of *PHIPA.*

Original Signed by: September 12, 2017

Lucy Costa
Investigator