Information and Privacy Commissioner,
Ontario, Canada

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

ORDER PO-4602

Appeal PA19-00565

Ministry of Health

February 4, 2025

Summary: A journalist made a request to the Ministry of Health (the ministry) for access to patient-level granular billing information for all Ontario physicians who billed for one million dollars or more during a specified time-period.

The ministry denied access to the requested information on the basis that it is personal health information under the *Personal Health Information Protection Act, 2004* (*PHIPA*) and *PHIPA* prohibits its release. In this order, the adjudicator upholds the ministry's decision and dismisses the appeal.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, as amended, sections 10(1) and 23; *Personal Health Information Protection Act, 2004,* SO 2004, c 3, Sched A, sections 4(1) and (2) (definitions of "personal health information" and "identifying information"), 8(1), 8(4) and 52.

Orders Considered: Orders MO-4166-I, PO-2744, PO-2811, PO-2892 and PO-3617.

OVERVIEW:

[1] The appellant, who is a journalist, was previously involved in an appeal before the Information and Privacy Commissioner (the IPC) where an order was issued directing the Ministry of Health (the ministry) to disclose the names, annual billing amounts, and medical field of specialization of the top one hundred physicians' billings to the Ontario

Health Insurance Program (OHIP) between 2008 and 2012.[1]

[2] This order considers a follow up request under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*)[2] made by the same journalist for patient-level billing amounts related to fee codes for all Ontario physicians who billed one million dollars or more for each fiscal year during a specified time-period.[3]

[3] In particular, the journalist asked for:

> … patient-level granular billing data for all physicians who billed for $1 million and up in any of the fiscal years in question [i.e. 2009/10 to 2013/14, inclusive, and all subsequent years available].
>
> Specifically, […] data on each patient visit (using anonymized descriptors for patients), including: date of patient visit, fee codes charged, and amount paid per fee code. (If it helps, this is the same kind of data provided on the top 100.)

[4] The journalist also suggested a manner of setting out the requested information:

> I suggest that your office provide the data [by] preparing a spreadsheet on each physician, as follows:
>
> Spreadsheet for Dr. X on Daily OHIP Data:

DATE	PATIENT SEEN (use anonymized descriptor)	FEE CODE	AMOUNT PAID PER FEE CODE

[5] The ministry issued a decision denying access to the responsive information. The ministry's decision stated that it was withholding the information for the following reasons:

> A search of the Health Insurance Division was conducted and after careful review of the data, it has been determined that with the granular level of

[1] Order PO-3617. This Order was upheld on judicial review in *Ontario Medical Association v. Ontario* (*Information and Privacy Commissioner),* 2017 ONSC 4090 (Ont. Div. Crt.) and subsequently in *Ontario Medical Association v. Ontario* (*Information and Privacy Commissioner*), 2018 ONCA 673, application for leave dismissed in *Ontario Medical Association, et al. v. Information and Privacy Commissioner of Ontario, et al.*, 2019 CanLII 29760 (SCC).

[2] RSO 1990, c F.31.

[3] The OHIP schedule of benefits identifies medical services that physicians can bill to the Ontario government. The fee that the government has agreed to pay physicians for performing each medical service listed in the schedule is identified by a specific code. The codes themselves are publicly available.

> the data being requested (including anonymized patient information, service dates, and fee schedule code information), the release may lead to the potential identification of a patient and/or patients.
>
> Please be advised that by providing physician names in conjunction with the data elements requested, it is reasonably foreseeable that a knowledgeable person would be able to link the information in the record to other information to identify individual patients. Due to the nature of the information in the record, and the small number of individuals/services involved, if released, could be used to identify one or more individuals. Therefore, this information is "personal health information" as that term is defined in Section 4 of the *Personal Health Information Protection Act, 2004* ("*PHIPA*"). Section 8(1) of *PHIPA* states that *FIPPA* does not apply to personal health information that is in the custody or under the control of a health information custodian, such as the Ministry. Accordingly, you do not have a right of access to this information under *FIPPA*.
>
> Furthermore, Section 52(1) of *PHIPA* only grants a right of access to personal health information to the person to whom the information relates.

[6] The requester (now the appellant) appealed the ministry's decision to the Information and Privacy Commissioner (the IPC). As a mediated resolution could not be reached, the appeal proceeded to the adjudication stage where an inquiry was conducted into the matter. Representations were then exchanged between the parties.

[7] In this order I uphold the ministry's decision to deny the access request and I dismiss the appeal.

RECORD:

[8] The records sought contain patient-level granular billing data for all physicians who billed one million dollars or more for the fiscal years 2009/10 to 2013/14, inclusive, and all subsequent years for which the data is available. Specifically, the data requested include the doctor's name, date of patient visit, the health card number for the patient seen (using an anonymized descriptor), the fee codes charged, and the amount paid per fee code.

DISCUSSION:

The right of access to the requested record is governed by *PHIPA*

[9] The appellant made the request under *FIPPA*. The ministry claims that the requested information constitutes personal health information to which the appellant has

no right of access under *PHIPA*.[4]

[10] *PHIPA* sets out rules governing access to records of personal health information, and the entitlement of a person to make a request for access to such records. Under section 52 of *PHIPA*, the right of access to personal health information belongs to the individual to whom the information relates.[5] *PHIPA* does not otherwise provide a general right of access to records of personal health information.

[11] However, as the ministry is subject to both *FIPPA* and *PHIPA,* if the information in the record qualifies as "personal health information," Sections 8(1) to (4) of *PHIPA* provide guidance regarding how *FIPPA* and *PHIPA* interact.[6] Sections 8(1) and (4) of *PHIPA* state:

> (1) Subject to subsection (2) [which is not relevant in these circumstances], the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* do not apply to personal health information in the custody or under the control of a health information custodian unless this Act specifies otherwise.
>
> (4) This Act does not limit a person's right of access under Section 10 of the *Freedom of Information and Protection of Privacy Act* or Section 4 of the *Municipal Freedom of Information and Protection of Privacy Act* to a record of personal health information if all the types of information referred to in subsection 4 (1) are reasonably severed from the record.

[12] What this means is that, under section 8(1) there is no right of access under section 10 of *FIPPA*[7] to records of personal health information in the custody or control of a health information custodian who is also an institution unless, as set out in the exception at section 8(4), all types of personal health information, as defined in *PHIPA,* can be reasonably severed from the record. Once all types of personal health information can reasonably be severed, access to the records can be considered under *FIPPA.*

[13] In this appeal, the ministry takes the position that because the record is a record of personal health information from which all types of personal health information cannot reasonably be severed even if anonymized descriptors are substituted for patient names and OHIP numbers, the exception at section 8(4) does not apply and as a result of the

---

[4] The ministry is subject to both *FIPPA* and *PHIPA* because it is both a health information custodian within the meaning of section 3(1) of *PHIPA,* and an institution within the meaning of section 2(1) of *FIPPA*.

[5] *PHIPA* also permits access by a "substitute decision-maker" who is a person authorized to make a request for access on an individual's behalf (*PHIPA*, sections 5(1), 23, 25).

[6] PHIPA Decision 30.

[7] *FIPPA* (Part II) grants an individual a right of access to records of general information. Section 10 of *FIPPA* reads: 10(1) Subject to subsections (1.1) and 69(2), every person has a right of access to a record or part of a record in the custody or under the control of an institution unless, (a) the record or part of the record falls within one of the exemptions under sections 12 to 22; or (b) the head is of the opinion on reasonable grounds that the request for access is frivolous or vexatious.

application of section 8(1), the appellant does not have a right of access to it under *FIPPA*. Accordingly, the ministry denies access to the information, in its entirety, on the basis that it is a record of personal health information to which the journalist has no general right of access under *PHIPA,* and which cannot be reasonably severed under section 8(4) to grant the appellant a residual right of access to the remaining information under *FIPPA*.

The requested record is a record of "personal health information" where the "personal health information" cannot be reasonably severed.

[14] To determine whether the appellant's right of access to the requested record under *FIPPA* is removed as a result of the application of section 8(1) of *PHIPA* or whether, the exception at section 8(4) applies to the record to grant the appellant a right of access under *FIPPA* to the information that remains once all the personal health information is removed, I must first determine whether the record at issue contains any "personal health information" as that term is defined in section 4(1) of *PHIPA* and if so, whether that personal health information can reasonably be severed.

Personal health information

[15] Personal health information is defined in section 4 of *PHIPA*, as follows:

> (1) "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,
> >
> > (c.1) is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the *Connecting Care Act, 2019*,
> >
> > (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
> >
> > (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
> >
> > (f) is the individual's health number, or

> (g) identifies an individual's substitute decision-maker.

[16] Section 4(2) defines "identifying information" referred to in section 4(1):

> (2) 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.

[17] Section 4(3) addresses identifying information that is not personal health information:

> (3) Personal health information includes identifying information that is not personal health information described in subsection (1) but that is contained in a record that contains personal health information described in that subsection.

[18] Considering the provisions set out above, information is personal health information only if it is "identifying information" about an individual - that is, the information must in itself identify the individual (for example, by consisting of the individual's name), or it must be reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify the individual.

Representations on whether the information at issue contains "personal health information" and whether any personal health information can be reasonably severed from the record

The ministry's representations

[19] The ministry submits that the record at issue contains personal health information as that term is defined in sections 4(1)(a) and (b) of *PHIPA* and because the personal health information cannot be anonymized, the record cannot be reasonably be severed to remove all personal health information.

[20] In support of its position, the ministry refers to Order PO-2744, in which the adjudicator referenced the *Guide to the Ontario Personal Health Information Protection Act,*[8] stating:

> … [In the *PHIPA* Guide], the authors examine an approach to determining whether information constitutes personal health information, and in

[8] The adjudicator cited: Perun, et. al., *Guide to the Ontario Personal Health Information Protection Act*, (Toronto: Irwin Law Inc., 2005) (*PHIPA* Guide).

particular, in determining whether the information is "identifying information" and whether it is "reasonably foreseeable in the circumstances" that the information could be used to identify an individual. The *PHIPA* Guide states, in part, at pages 76-79 (footnotes omitted):

> …The issue of whether particular information constitutes identifying information is not always black and white. "Data identifiability can be characterized as a continuum or sliding scale, in which the divisions between degrees of "identifiability" and "anonymity" are not always clear cut."
>
> …[I]t is probable that it is reasonably foreseeable in the circumstances that information can be used to identify an individual when the recipient of the information is known to have access to other information that, when combined with the information that it received, would identify the individual to whom the information relates… As a result, it is necessary to consider the resources of the recipient of the information.
>
> …The collection of certain data elements may increase the likelihood of a patient being identified. These data elements include the following:
>
> - geographic location (e.g., location of residence, location of health event, especially where the location is not heavily populated);
> - names of health care facilities and providers
> - rare characteristics of the patient (e.g. unusual health condition); or
> - highly visible characteristics of the patient (e.g., ethnicity in certain locales).
>
> In the context of [*PHIPA*], the [IPC] has supported a conclusion that the "identifiable" threshold may be met where the information to be disclosed would lead one to identify a group of fewer than five individuals to whom the information may relate … [and] has also had the opportunity to consider the impact of one data element, the postal code, on the identifiability of an individual …

[21] The ministry submits that the breadth and granular level of the data elements requested increases the likelihood of a specific patient being identified or the likelihood that a physician is identified as a provider of a particular health care service to a specific patient. The ministry says that this is so even where an anonymized descriptor is used

for a patient instead of an OHIP number because the data elements include the following:

- the fee code which would reveal the treatment or service the health care provider provided to the patient, as well as the health care provider's specialty, which may also reveal a very sensitive health condition of a patient and as outlined below, may also reveal other specific characteristics of the patient;

- the name of the health care provider that provided the treatment or service to a patient; and

- the date the health care provider provided the treatment or service to a patient, of which there are many days where a specialized treatment or service would be provided to only a small number of individuals. (Note: the opportunities for re-identification are greatly increased by releasing these data elements by service date rather than by releasing them as aggregated data on an annual basis).

[22] Furthermore, the ministry submits that the particular data elements requested, such as the fee code, may also increase the likelihood of revealing additional attributes about a patient and/or the treatment or service they received from a particular health provider:

- The sex of a patient may be inferred from certain fee codes that relate to sex-specific services such as certain surgical procedures or family planning services. For example: fee codes relating to antenatal care would indicate female patients whereas fee codes relating to testicular concerns relate to males. Several hundred sex-specific fee codes exist within the Schedule of Benefits.

- The age and/or age range of a patient may be inferred from certain fee codes that are for services or treatments that are specific to newborns, children, adolescents or seniors. In addition, some fee codes, such as those associated with pap testing, mammography and colonoscopy are all associated with age restrictions that would assign an individual patient to a specific age range.

- The type or nature of care a patient received may be inferred from certain fee codes that would reveal the department or how a patient received a service or treatment. For example, fee codes may indicate that care was provided in the intensive care unit or the emergency department or may indicate that the patient received treatment on an in-patient or out-patient basis.

- The time of day a patient received the treatment, or service may be inferred from certain fee codes, such as specific fee codes for after hour premiums or surgical start time premiums.

- The location of where a patient received service or treatment could be inferred by using the name of the physician in conjunction with a physician's practice address,

> which is easy to determine through public resources such as the doctor search on the College of Physicians and Surgeons website.

[23] The ministry asserts that asking for all record-level claims data of physicians who billed more than one million dollars for the time-period requested would greatly increase the likelihood of a patient being identified or the likelihood that a physician is identified as a provider of health care to a specific patient because of the inherently unique data profile that may be generated from this extensive dataset. The ministry submits that:

> The requested dataset would result in a dataset of hundreds of millions of datapoints about patients. Each record-level entry for a patient reveals a point of information about an individual that can be compiled into a potentially unique data fingerprint, thus resulting in the increased likelihood of re-identification even where an anonymized descriptor for a patient is used. The more expansive the dataset is - in terms of its breadth of data attributes and/or its longitudinal depth - the higher the probability is that the contained datapoints could be used for the successful reidentification of patients.

[24] In addition, the ministry states that in some instances, a small number of individuals received a particular type of service or treatment, which would further increase the likelihood of potential identification of patients who received that service. The ministry submits that in previous IPC orders, such as Order PO-2811, the IPC explained that the term small cell count refers to a situation where the pool of possible choices to identify a particular individual is so small that it becomes possible to guess who the particular individual might be, and the number that would qualify as a small cell count varies depending on the situation. In Order PO-2811, the adjudicator described the term "small cell" count and the ministry's misapplication of it in that case in the following way:

> [The] Ministry submits that there are five or fewer registered sex offenders residing in 45% of Ontario's FSAs [Forward Sortation Areas or areas defined by groupings of postal codes]. The Ministry submits that this comprises a "small cell" count. The term "small cell" count refers to a situation where the pool of possible choices to identify a particular individual is so small that it becomes possible to guess who the individual might be, and the number that would qualify as a "small cell" count varies depending on the situation. The Ministry has misapplied the concept of "small cell" count here. If, as the Ministry argues, 5 individuals is a "small cell" count, this would mean a person was looking for one individual in a pool of 5. By contrast, the evidence in this case indicates that one would be looking for 5 individuals in a pool of anywhere from 396 to 113, 918 [the range of populations of the FSAs]. This is not a "small cell" count.

[25] The ministry submits that some of the numbers at issue in this appeal (the number of services provided by the physician per day) would qualify as a small cell and that the

relevant pool is the same size. It submits that, based on the wording of the request, the relevant pool consists of the number of people who have received a type of treatment by the physician on a specific date. The ministry submits it is reasonably foreseeable in the circumstances that the disclosure of this information could be used to confirm a patient's identity or the identity of their provider, and more importantly, that they received a particular type of treatment during the specific time period.

[26] The ministry further submits that given the time frame of the request (which spans many years), the longitudinal nature of the data increases the likelihood that the combination of data elements being sought at the individual record level can be "compiled into a potentially unique data fingerprint", which greatly heightens the risk of linking and re-identification.

[27] In support of its position that the responsive records could be used with other available information to identify a patient over time, the ministry provides the following examples:

> Example 1. The family physician of a family of three (2 parents + 1 teenager) is amongst the cohort of physicians who have billed more than 1 million dollars in several consecutive fiscal periods.
>
> - The parents have pre-existing knowledge of the service dates when all three members of the family attended the physician's office together for influenza vaccination over multiple years.
>
> - By evaluating the record-level claims data, the parents are able to identify three unique health cards that were billed for immunization services by the physician on the known service dates.
>
> - No other "three health card clusters" with the same data attributes are found within the dataset (same physician, same service dates, same fee codes).
>
> - The parents with knowledge of their own medical services history, are able to identify themselves from the three health cards cluster, thus identifying the health card number of their teenager through the process of elimination.
>
> - The parents - now with knowledge of their teenager's anonymized health card number – can query the dataset by health card number.
>
> - They find that the health card is linked to service claims by another physician for addictions counseling codes.

> Example 2. While gossiping in the lunchroom, an employee mentions to their employer that two of their physicians were amongst the list of providers billing more than 1 million dollars per year.
>
> - The employer requires that all employees provide a sick note when absent from work due to illness.
>
> - Out of curiosity, the employer utilizes information contained on historical sick notes submitted by the employee to identify the names of the employee's physicians.
>
> - The employer confirms that two physicians named on the sick notes are amongst the cohort of physicians who have billed more than 1 million dollars in a fiscal year.
>
> - Using historic sick notes from the two different physicians as markers for service date, the employer identifies a single health card associated with claims by the respective physicians on the respective dates of service.
>
> - The employer uses additional sick notes to cross- reference claims associated with the identified health card number, thus increasing the probability of successful reidentification.
>
> - The employer - now with knowledge of their employee's anonymized health card number - queries the dataset by health care number. They find that the health card is linked to services claims for mental health counseling codes.

[28] The ministry submits that these two examples highlight that even a collection of ordinary record-level data points in a dataset of sufficient longitudinal span can enable the successful re-identification of individuals. It submits that this reflects an inherent statistical fact that cannot be overcome by routine de-identification procedures (e.g. the removal of rare fee codes, etc.).

[29] In its representations, the ministry provides a third example which it characterizes as a "real-world example" to illustrate its position that it is reasonably foreseeable that an individual could use the responsive records combined with other information to identify a patient:

> The following is a real-world example. The attached newspaper article reported the occurrence of a COVID-19 death at Kingston General Hospital and the name of the deceased. The article indirectly indicates the date of admission and the date of death. Using service dates and knowledge of death pronouncement fee codes and ICU fee codes, it is possible to reduce the population of possible individuals from responsive records to a single

> individual, thereby revealing personal health information about the individual named in the newspaper article.[9]

[30] The ministry adds that even if anonymized descriptors are used in the place of patient names, it would be reasonably foreseeable in the circumstances that the responsive records could be utilized with other information to identify an individual. This is because of the combination of the granular level data elements requests and the breadth of the data set requested:

> If patients were identified with different anonymized descriptors for each visit or for each service provider, the Ministry submits that the responsive records would still be considered identifying information for the same reasons described above. Severing linkages in this manner would reduce the ease by which re-identification may be accomplished and would attenuate the harm of a successful attack but it would not eliminate that harm. Instead, this method would provide re-identification opportunities on a smaller scale and would not ensure that individuals are adequately protected against intrusions on their personal health information.

[31] The ministry states that it has no knowledge as to whether the appellant will use the information at issue to identify the individual patients who received the services but is concerned with the potential release of the information into the public domain. The ministry submits, if released, the responsive records, which contain hundreds of millions of datapoints, could be combined with other information that is available to the public and used for any purpose.

The appellant's representations

[32] The appellant emphasizes that they do not have any interest in accessing personal patient information and suggests an alternative way of presenting the data so that the ministry's concerns are addressed. They suggest that, for every doctor, the ministry use different anonymized identifiers in place of patient names and OHIP numbers. They submit that if this approach were taken, someone in possession of the data would not be able to identify all of the different physicians that a single patient was seeing. They submit that they would be open to exploring with the ministry other ideas to manipulate the data address the ministry's concerns about re-identification. The appellant submits that they are open to having the ministry exclude data relating to abortions and Medical Assistance in Dying (MAID). They also submit that they are willing to narrow their request to a single year's worth of data, the most recent year available.

[33] The appellant notes that in 2019 they were provided the same level of granular data on the top-100 billers and "understand[s] that the ministry, in hindsight, believes it provided too much data to [them]." They submit that no patients were ever identified

[9] The ministry provided a link to the article in its representations.

from that data even though it was used to create a number of stories, graphics and public databases which ran under the title: Operation Transparency.[10]

[34] The appellant states that their interest in seeking more data of a similar nature is to produce more of this type of journalism. They explain that their ultimate goal is to take a close look at the province's spending on physicians and on the provision of tests, treatments and procedures to patients.

[35] The appellant adds:

> This kind of journalism is done in the public interest. We can see how limited health-care dollars are allocated. And we can look, for example, at whether too many of specific services are being done (similar to the work of the Choosing Wisely campaign).
>
> Given these are taxpayer dollars at stake, the public should have a right to see how they are being spent. The granularity of the data helps with doing investigative journalism.

[36] The appellant submits that in one of their earlier appeals with the IPC, the appeal resolved in Order PO-3617, the adjudicator ordered the ministry to disclose the names of the top-100 OHIP billers along with "data on their compensation from the province." They submit that this order and related court decision on subsequent appeals contain information about "the value of making public data related to provincial payments to physicians."

The ministry's reply

[37] In response to the appellant's suggestion that anonymized descriptors be used instead of patient names and OHIP numbers, the ministry submits that patients could still be identified (as shown by the examples above).

[38] With respect to the appellant's willingness to remove data relating to abortions and MAID from the scope of their request, the ministry submits that:

> … while that particular subset of data could be excluded, that would not change its position with respect to the rest of the dataset. For the residual dataset that would continue to be within the scope of the appellant's request, there would remain the risk of re-identification for any patient who has received other medical services/procedures for the reasons noted in the Ministry's initial representations and these reply representations.

[39] Finally, with respect to the appellant's suggestion about narrowing the scope of the request to just a single year's worth of data, the ministry submits that this does not

[10] The appellant provided a link to this information in their representations.

change its position because of the nature and breadth of the data elements being requested:

> … Even if the dataset were narrowed to a single year, using previous FY data for all physicians and all claims (i.e. averaging out 5 physicians and their claims totals for the year), for all 31,000 physicians, the Ministry estimates that a full fiscal year of data would encompass roughly 1.8 billion rows of data. This is only a rough estimate based on averages, but the Ministry submits that it provides a snapshot of how comprehensive the data points are. As indicated in the Ministry's initial representations, each record-level entry for a patient reveals a point of information about an individual that can be compiled into a potentially unique data fingerprint, thus resulting in an increased likelihood of reidentification even where an anonymized descriptor for a patient is used. At paragraphs 9 and 10 of the Ministry's initial representations, the Ministry explained what could be revealed or inferred about patients from various datapoints. As the IPC stated in Order PO-2744, the "collection of certain data elements may increase the likelihood of a patient being identified" and this is applicable in this current appeal.

[40] The ministry submits that because of the granular nature of the data, even with anonymized patient information per individual physician, it is reasonably foreseeable in the circumstances that the information could still be used to confirm a patient's identity, and more importantly, that they received a particular type of treatment during the specific time period.

[41] The ministry submits that:

> It has consistently been the Ministry's position that when a physician's name (and location can be easily found with name), date of service, and fee code are provided together, it is possible through social media, news, and other means to use this information to potentially identify an individual patient. Subsequently, any other data that is released can be linked with already-available data. As more data is released (and becomes publicly available), there is more risk of linkages in future data requests as there is more in the public domain to cross-reference.

[42] Finally, the ministry acknowledges that in hindsight it believes that too much data was provided in that previous request and, even if no patients have been identified as the appellant asserts, it acknowledges that this prior data release was considered when it made its decision in this current appeal.

[43] The ministry notes that previous orders issued by the IPC have established that

disclosure to a requester is considered "disclosure to the world."[11] It submits that it considered this principle in the context of the current appeal, "especially in light of the existence of the public database containing physician billing data on the [appellant's media outlet's website]."

Analysis and finding on whether the record contains "personal health information" as that term is defined in Section 4(1) of PHIPA.

[44] To qualify as "personal health information" under section 4(1) of *PHIPA*, it must be "identifying information about an individual". Section 4(2) of *PHIPA*, which is reproduced above, defines "identifying information" as "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." Therefore, to determine whether the record contains personal health information, I must determine whether it is reasonably foreseeable that an individual or individuals could be identified by the disclosure of the information in the sample record alone, or in combination with other available information.

[45] The data requested by the appellant includes the doctor's name, date of patient visit, an anonymized descriptor instead of the patient's name or health card number, the fee code for the service and the amount paid per fee code. This information is personal health information as it is identifying information about an individual relating to providing of heath care to the individual, including the identification of a person as a provider of health care to the individual as set out in section 4(1)(b).

[46] However, the appellant clarified that she was not seeking access to the personal health information of any identifiable individual and suggested that unique anonymized identifiers that are different for every doctor be used in place of patient health card numbers.

[47] The ministry takes the position that even if certain information in the record were anonymized in the manner suggested by the appellant, the record still contains personal health information within the meaning of that term in section 4(1) because the information is "identifying information" as defined in section 4(2). The ministry argues that is reasonably foreseeable the information in the record could be combined with other available information to identify individual patients in connection with a particular health condition or treatment (section 4(1)(a)) or a physician listed in the report as a provider of health care to a particular patient (section 4(1)(b)).

[48] For the reasons set out below, I agree with the ministry and find that the information requested by the appellant is personal health information within the meaning of that term in Section 4 of *PHIPA*. Having considered the representations before me as well as the information in the sample record, I accept that, were the specific data points

[11] The ministry cites, for example, Orders MO-3730-R, PO-2018 and PO-3140.

sought by the appellant disclosed, even if the patients name or health card number were anonymized as suggested by the appellant, it is reasonably foreseeable that they could be combined with other available information to identify an individual.

Identifiability

[49] In coming to the conclusion that an individual could be identified were the specific information requested by the appellant disclosed, I have considered Interim Order MO-4166-I. In that case, a district health unit argued that while daily summaries containing reporting information about COVID-19 cases did not contain information that could be construed as "personal health information" under *PHIPA*, if those daily summaries were modified from a district level to a municipal level (which was the format requested), disclosure of this modified information could lead to an individual being identified. Because the modified information was not contained in any records before her, the adjudicator reserved her finding on the issue of identifiability in that case. However, she provided general guidance to the district health unit to help it assess whether disclosure of the modified information being requested would result in identification, pointing to prior IPC and court decisions, and other resources addressing "identifiability" and "small cell count."[12]

[50] In Order PO-2892, former Commissioner Brian Beamish[13] made statements on the issue of identifiability resulting from combining the information being sought with other information in the public realm. He determined, however, that this did not affect a decision to disclose such records since he concluded that the disclosure of the anonymized information itself would not result in unnamed individuals being identified.

[51] I agree with the guidance provided by the adjudicators in the orders cited above on the issue of identifiability and take a similar approach in my determination of whether the record contains identifying personal health information.

[52] The information in the sample record, if not anonymized at all, contains a great deal of information that could lead to the identification of a patient, notably a patient's health card information. However, even if individual names and OHIP numbers are replaced by anonymized codes as suggested by the appellant, and the data related to abortions and MAID are removed and the data is limited to a year, I have been provided with sufficient evidence to conclude that it is reasonably foreseeable that the disclosure of the information being requested when combined with other available information would lead to the identification of patients.

[53] The ministry has provided several concrete examples of how this could happen. In

---

[12] The threshold that is often referred to in these orders is a "cell size of five". At section 6 of Health Canda's guidance document for public data release entitled "Public Release of Clinical Information: guidance document - Canada.ca" the "cell size of 11" is mentioned as an appropriate threshold. The 2016 IPC De-Identification Guidelines for Structured Data discusses a threshold from 10 to 20.

[13] He was Assistant Commissioner when he issued Order PO-2892.

my view, the examples are not far-fetched or fanciful but demonstrate how vast amounts of specific datapoints, when combined with other data already known to others, or already disclosed (including the billing information previously disclosed as a result of Order PO-3617), can lead to identification. If combined with the name of a doctor, date of visit and possible geographic location, which can be discerned through the location of a doctor's office or hospital where the doctor may have privileges, re-identification may occur. I also note that there are conditions, diseases or treatments that may be sufficiently rare or the known prevalence of a specific procedure or diagnosis that is within a doctor's known specialization such that they could be more readily inferred with a fee code and matched with information that is already known or highly visible to others, for example amputation or a condition requiring a physical device.

[54] I have also considered the possibility of severing information as suggested by the appellant, however, the ministry has persuaded me through several credible examples that even in the anonymized form suggested by the appellant, identification would still be reasonably foreseeable.

[55] I find therefore that the record at issue is a record of personal health information governed by *PHIPA*. As this personal health information does not belong to the appellant, she has no general right of access to it under *PHIPA.*

The record is not reasonably severable within the meaning of Section 8(4) of PHIPA

[56] Although the appellant does not have a general right of access to the record under *PHIPA*, as stated above, because the ministry is also an institution subject to *FIPPA*, if the personal health information in the record is reasonably severable, pursuant to section 8(4) she may have a right of access under *FIPPA* to the information that remains once all the personal health information has been severed.

[57] I found above that even were the report anonymized in the manner suggested by the appellant, the record remains personal health information. From my review of the sample record, I find that it is not possible to reasonably sever the record as contemplated by section 8(4) of *PHIPA*, because in my view, there is nothing other than personal health information in it. As the record is not reasonably severable within the meaning of section 8(4) of *PHIPA* the appellant has no right of access to it under *FIPPA*.

[58] In reaching my finding in this order, I considered all of the arguments made by the appellant including the purpose for which she intends to use the information. In particular I note that the appellant argues there is a public interest in the disclosure of the record. To this end, it appears that the appellant may be attempting to raise the possible application of the public interest override at section 23 of *FIPPA.* Section 23 permits information to be disclosed if there is a compelling public interest in disclosure of the information that clearly outweighs the purpose of the applicable exemption under *FIPPA.* As the appellant does not have a right of access under *FIPPA* to the requested

record, section 23 has no application in this appeal. Additionally, I note that there is no equivalent public interest override provision in *PHIPA*, and public interest considerations are not relevant to the question of reasonably severability under section 8(4) of *PHIPA*.[14] Accordingly, I find no basis for reading in a public interest override that would confer a right of access under *PHIPA* where there otherwise is none.

Conclusion

[59] For the reasons set out above, I find that the appellant does not have a right of access to the requested information under either *PHIPA* or *FIPPA*. As a result, I uphold the ministry's decision and dismiss the appeal.

ORDER:

I uphold the ministry's decision to deny access to the information sought by the appellant and I dismiss the appeal.

Original Signed by:	February 4, 2025
Steven Faughnan Adjudicator	

[14] PHIPA Decision 27.