Manitoba Ombudsman

REPORT UNDER

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

CASE 2013-0228 (web version)

MANITOBA HEALTH

ACCESS COMPLAINT: REFUSAL OF ACCESS

PROVISIONS CONSIDERED: 2, 3(a), 6(2), 7(1), 7(2), 17(1), 17(2)(a), definition of "personal health information"

OTHER RESOURCES CONSIDERED:
HIPAA Privacy Rule and "Safe Harbour" Standard
Pan-Canadian De-identification Guidelines for Personal Health Information

REPORT ISSUED ON OCTOBER 22, 2013

SUMMARY: The complainant requested access to all records pertaining to the Discharge Abstract Database and the National Ambulatory Care Reporting System, advising that she was not interested in obtaining access to any personal information contained in those records. The public body declined to provide the complainant with any information from the records, considering the patient-level data in the records to be personal health information of third parties that could not reasonably be severed from the records. We found that the information was personal health information that was required to be withheld and that it could not reasonably be severed to provide access to residual fields of data for the approximately 600,000 patient-level records that were within the scope of the request.

THE COMPLAINT

On April 29, 2013 under *The Freedom of Information and Protection of Privacy Act* (FIPPA or the act), the complainant requested access to the following information:

> All records pertaining to the Discharge Abstract Database and the National Ambulatory Care Reporting System for acute care hospitals in Manitoba, submitted to the health ministry and/or the health minister and/or Manitoba hospitals by the Canadian Institute for Health Information for the most recent reporting year. I am not interested in personal information about patients that may be contained in the records. As such, any personal identifiers contained in the records should be removed.

Manitoba Health (the public body) responded to the request on May 29, 2013, refusing access in full under section 17 of FIPPA on the basis that the information requested is personal health information of third parties that is required to be withheld under FIPPA. Manitoba Health indicated that the information could not reasonably be severed to remove data that might identify individuals.

A complaint about refused access was received by the ombudsman on July 3, 2013. The complainant advised that she was aware of the need to protect personal privacy and that is why she specifically requested anonymized data. She believed that, after removing personal identifiers from the records, it would take an extraordinary effort to identify individuals. As such, she felt that the public body could provide access to the remaining information.

THE POSITION OF MANITOBA HEALTH

Manitoba Health's response letter relied on section 17 of FIPPA to refuse access in full, advising that the Discharge Abstract Database (DAD) and the National Ambulatory Care Reporting System (NACRS) are databases containing line level data (or personal health information), and that *The Personal Health Information Act* (PHIA), and not FIPPA, governs the disclosure of personal health information.

Manitoba Health indicated that the access request was received under Part 2 of FIPPA – Access to Information and referred to PHIA's Part 3 - Protection of Privacy, in its response letter to the complainant. Manitoba Health maintained that, in order to appropriately protect and safeguard the information contained in DAD and NACRS, it was required to look to PHIA as the governing legislation. It held that requests for access to large amounts of raw, line level data should be considered requests for "health research," and that such requests fall outside of the scope of FIPPA. In this regard, the public body emphasized that certain provisions under PHIA deal specifically with "disclosures for health research," and that these provisions are intended to ensure that personal health information is used for research purposes only and that reasonable safeguards are in place to protect the confidentiality and security of the personal health information.

The public body referred the complainant to a process established under PHIA for obtaining information through the Health Information Protection Committee (HIPC) and advised that this process was established for individuals or groups conducting health research to gain access to records containing personal health information. It explained that research is approved when HIPC considers the importance of the research outweighs the intrusion into privacy and then determines whether sufficient safeguards are in place to protect the confidentiality of the information. The public body provided the complainant with the website address to obtain more information regarding this process. Additionally, Manitoba Health advised the complainant that she could partner with a researcher, having the appropriate designations, in order to meet the criteria set by HIPC.

During the course of our investigation, Manitoba Health indicated that it had considered several options before reaching its final decision to refuse access. The public body advised that, for the

most recent reporting year, DAD held approximately 250,000 records and NACRS held approximately 325,000 records, with each record containing approximately 600 fields. According to Manitoba Health, attempting to sever those records to provide only that information not considered to be personal health information would require significant manual review and programming and computer processing resources, such that processing the request would unreasonably interfere with its operations.

Manitoba Health believed that this information could not reasonably be severed from the records and, in this regard, refused access in full under subsection 17(1) and clause 17(2)(a) of FIPPA, provisions that except personal health information of third parties from disclosure.

PRELIMINARY MATTERS - BACKGROUND

Scope of FIPPA

We considered the following general provisions of FIPPA to be relevant to our investigation:

> **Scope of this Act**
> **3** This Act
> (a) is in addition to and does not replace existing procedures for access to records or information normally available to the public, including any requirement to pay fees;
>
> **Part does not apply to publicly available information**
> **6(2)** This Part does not apply to information that is available to the public free of charge or for purchase.

Purpose and Right of Access Under FIPPA

Of significance to this request is that the right of access (corresponding with the purpose) extends to any record in the custody or control of a public body, but does not extend to information that is excepted from disclosure, nor the remainder of the information in the record, if the excepted information cannot reasonably be severed from the record.

Clause 2(a) and Subsections 7(1) and 7(2) are relevant:

> **Purposes of this Act**
> **2** The purposes of this Act are
> (a) to allow any person a right of access to records in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act
>
> **Right of access**
> **7(1)** Subject to this Act, an applicant has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.

> **Severing information**
> **7(2)** The right of access to a record does not extend to information that is excepted from disclosure under Division 3 or 4 of this Part, but if that information can reasonably be severed from the record, an applicant has a right of access to the remainder of the record.

Under section 17 of FIPPA, personal health information is excepted from disclosure. The respective provisions are as follows:

> **Disclosure harmful to a third party's privacy**
> **17(1)** The head of a public body shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's privacy.
>
> **Disclosures deemed to be an unreasonable invasion of privacy**
> **17(2)** A disclosure of personal information about a third party is deemed to be an unreasonable invasion of the third party's privacy if
> (a) the personal information is personal health information

Personal health information is defined under FIPPA (and PHIA) as:

> **"personal health information"** means recorded information about an identifiable individual that relates to
> (a) the individual's health, or health care history, including genetic information about the individual,
> (b) the provision of health care to the individual, or
> (c) payment for health care provided to the individual,
> and includes
> (d) the PHIN as defined in The Personal Health Information Act and any other identifying number, symbol or particular assigned to an individual, and
> (e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care

Canadian Institute for Health Information (CIHI)

The Canadian Institute for Health Information (CIHI) is a national not-for-profit organization whose mandate, according to its website, is "to lead the development and maintenance of comprehensive and integrated health information that enables sound policy and effective health system management that improve health and health care." CIHI is one of only two prescribed health research organizations recognized under PHIA, and receives datasets of health service information from provincial health ministries, including Manitoba Health. These datasets are provided pursuant to a formal agreement between Manitoba Health and CIHI. CIHI, in turn, analyzes and generates data that are comparable across the country. References to CIHI in this report are based on information available on the CIHI website in most cases, although some information has been provided by Manitoba Health.

The Discharge Abstract Database and the National Ambulatory Care Reporting System

The Discharge Abstract Database (DAD) and the National Ambulatory Care Reporting System (NACRS) are two of the core clinical administrative databases at CIHI. DAD contains data for hospital impatient acute discharges and, in some cases, chronic, rehabilitation and day surgery separations from health care facilities; NACRS contains data on emergency and ambulatory care visits, such as those at day surgery and outpatient clinics.

Manitoba Health and Health Information Management

Health Information Management is a program area of Manitoba Health. One of HIM's objectives is to coordinate and support health research-related activities, and ensure the appropriate use of health information in accordance with privacy legislation. Provincial Health Records Management, an area within HIM, supports DAD and NACRS datasets which are reported nationally to CIHI.

ANALYSIS OF ISSUES AND FINDINGS

1. Is the requested information available through an existing procedure for accessing records/information generally available to the public?

Section 3 of FIPPA indicates that FIPPA does not replace existing procedures for accessing records/information normally available to the public. In fact, subsection 6(2) of the act indicates that the formal access request process does not apply to information that is available to the public free of charge or for purchase.

Based on our review of information available on CIHI's website and information provided by Manitoba Health, we learned that there are existing procedures for accessing health information datasets for research through HIPC and/or for research and other purposes through CIHI.

As previously noted, information for an approved research purpose may be available through HIPC, but only if certain conditions are met. Similarly, CIHI has processes in place to provide access to publicly available data as well as more detailed information. CIHI staff are educated and trained in the area of what constitutes personal health information and, in the event of a request for detailed or potentially identifying health information, requesters are required to submit a custom data request using CIHI's Data Inquiry Form, and must also sign Non-Disclosure/Confidentiality Agreements.

Manitoba Health produces annual statistics that are available to the general public. Similarly, the information that is publicly available on CIHI's website is statistical information. Access to information beyond these parameters is only available in select circumstances and to select roles within the health-care system, and strict limits are imposed on what researchers can do with the information, in order to protect the privacy of individuals whose personal health information is contained in the data sets.

While we agree that there are existing procedures for accessing health information data through HIPC and/or by contacting CIHI, we do not find that the information as requested by the complainant is that which would normally be available to the "public" through either of these processes. Additionally, these processes are not equivalent to the broad right of access under FIPPA, which places no limits on what an applicant may do with the data.

2. Is the information in question required to be withheld under section 17 of FIPPA?

Section 17 of FIPPA sets out a mandatory exception to the broad right of access, in order to protect the personal information of third parties. Subsection 17(1) prohibits a public body from disclosing personal information if it would be an unreasonable invasion of a third party's privacy.

Subsection 17(2) of FIPPA provides a list of those types of information that are so sensitive that their disclosure is deemed to be an unreasonable invasion of privacy. The first type of information on that list is personal health information.

The records at issue in this case are records of personal health information, the type of information that is required to be withheld under subsection 17(1) and clause 17(2)(a) of FIPPA. The information in these records cannot be released, unless the records can reasonably be severed to remove any data that would identify individuals that are the subjects of patient-level records.

3. Can the excepted information reasonably be severed from the records so that the remaining information cannot be linked to identifiable individuals?

The complainant's request indicated that she was not interested in obtaining personal information about patients and that "any personal identifiers" in the records should be removed. We will now consider whether the records can reasonably be severed. When dealing with personal health information data, this process is commonly known as "de-identification." Data is de-identified when it is stripped of information so that the data subject cannot be identified. For example, in health research, data is stripped of elements that could identify the individual patient or research participant. Given the sensitivity of health information and the importance of health information datasets to research, de-identification procedures or frameworks have been developed and have been adopted in the research and health services sectors. Following is our consideration of the principles found in select de-identification frameworks and their relevance/application to the information at issue in this request.

The U.S.'s *Health Insurance Portability and Accountability Act* (HIPAA) Privacy Rule and the "Safe Harbor" Privacy Framework

For purposes of this investigation, we felt it important to highlight the process or "privacy framework'" for protecting health information maintained in the U.S., which is subject to regulation under HIPAA. The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. The Privacy Rule calls this information

protected health information (PHI). The definition of PHI includes the phrase, "*that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual."* The Privacy Rule provides a de-identification standard to allow use and disclosure of information that neither identifies nor provides a reasonable basis to identify an individual. The methods available under the Privacy Rule yield de-identified data that retains some risk of identification. Although the risk is very small, it is not zero, and there is a possibility that even properly de-identified data may still be linked back to the identity of the individual to which it corresponds. One method of meeting the requirements of the Privacy Rule involves the use of expert analysis developed specifically for the data in question. We discuss the other, perhaps more well-known, method next.

Satisfying HIPAA's "Safe Harbor" Standard for De-identifying Data

A method exists under the Safe Harbor Standard to determine if information is adequately de-identified. Firstly, the following identifiers of the individual or of relatives, employers, or household members of the individual are removed. Parts or derivatives of any of the listed identifiers may not be disclosed.

- Names
- Addresses, except for some digits of the ZIP code
- Dates, except years, for dates that are directly related to the individual
- Telephone numbers, fax numbers, email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License Numbers
- Vehicle identifiers, serial numbers, license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators
- Internet Protocol addresses
- Biometric identifiers, including finger and voice prints
- Full-face photographs and any comparable images
- Any other unique identifying numbers, characteristics, or codes (exceptions apply), for example clinical trial record numbers, occupations.

Secondly, the "entity" must not have actual knowledge, i.e., clear and direct knowledge, that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

Pan-Canadian De-Identification Guidelines for Personal Health Information

Much has been written about the capabilities of individuals with certain analytic and quantitative capacities to combine information in particular ways to identify health information. In Canada, experts at the Children's Hospital of Eastern Ontario (CHEO) Research Institute and the

Associate Professor in the University of Ottawa's Faculty of Medicine, with Research Ethics Board approval, set out to attempt to reverse de-identified data and assess existing flaws in security protocols. What resulted from that research project was a report titled *Pan-Canadian De-Identification Guidelines for Personal Health Information* (which we will refer to as the guidelines). The guidelines describe some of the ways in which data can be re-identified using analytical tools in conjunction with information already available from various sources about particular populations. The report also speaks about the principles, metrics and methods that can be used to manage the privacy risks associated with disclosing data.

Based on our review of the guidelines, it appears that the de-identification process would generally begin with consideration of certain variables from the data, which are referred to as identifiers and quasi-identifiers (similar to the identifiers listed for the HIPAA Safe Harbor method). Importantly, the guidelines indicate that whether a variable is an identifier, quasi-identifier or non-identifier will vary, depending on the distribution and uniqueness of characteristics among individuals whose information makes-up the data-set. Variables that are clearly identifiers are to be removed from the data, randomized, or coded. Variables that are generally considered to be quasi-identifiers and variables that might exist in available datasets or databases are to be flagged and quantitative analysis undertaken of the likelihood of re-identification associated with individual variables and combinations of variables. This analysis is meant to identify risk thresholds associated with failing to remove variables (singly or in combination). Depending on the risk threshold, further analysis would need to be undertaken, using what the guidelines refer to as "Quantitative Disclosure Control Techniques."

It is important to note that these techniques reduce but do not entirely eliminate the risk of re-identification. It is our understanding that the objective of quantifying the remaining risk in any particular situation is for the purpose of weighing the risk against the anticipated benefit and then making a determination about whether to proceed with releasing the information.

Manitoba's Privacy Legislation and the Right of Access in Terms of Reasonableness of Severing

Manitoba's privacy legislation stringently protects personal health information and the definition of personal health information provided in FIPPA and PHIA does not address the issue of there being a "reasonable basis" for identifying an individual, nor provide a method for determining whether an individual is identifiable.

It is clear to our office that a significant number of data fields would need to be severed from the datasets before Manitoba Health could even consider releasing the data in question. In our view, the department would have to withhold all demographic fields that could potentially identify an individual. This would include such information as PHIN, birth date, gender and postal code. In order to further reduce the risk of re-identification, hospital identifiers would also need to be severed as this, together with diagnoses, conditions, treatments, and dates of admission and discharge could potentially identify a patient. Physician identifiers could also link back to identifiable individuals.

Of particular difficulty in this case is that for each of the almost 600,000 patient-level records, there are roughly 600 fields of data, with over 100 fields of diagnosis-related information alone

for each record. Even when major identifiers, such as postal code and date of birth, are removed, many minor identifiers, individually non-identifiable, can render individuals identifiable, especially when information such as diagnosis, hospitalization dates, procedures, or treatments might be unique to one individual or to a small number of individuals. Based on our consideration of the de-identification standards discussed earlier in this report, our office would agree that even after severing specific fields of data, Manitoba Health would need to conduct a significant additional manual review and analysis to determine whether remaining data fields could be used to potentially re-identify patients.

What this means is that any remaining information, after conducting a manual review, is not necessarily non-identifiable; that would depend on whether and what other information is or has been made available. We note that if this type of residual information were to be released by CIHI for health research or health system analysis purposes, the risk would be managed by way of a confidentiality agreement with the researcher or health manager. No such measures are available to protect information released by Manitoba Health in response to a FIPPA request, as the act does not provide for conditions to be imposed by a public body on what an applicant can do with information once released.

It is our view that is not reasonable for Manitoba Health to review and sever the records, such that the only information that would remain would be, as requested by the complainant, information that is not personal information.

We find, therefore, that the right of access does not extend to the information requested by the complainant by virtue of subsection 7(2) of FIPPA - the personal health information excepted from disclosure under subsection 17(1) and clause 17(2)(a) of the act cannot reasonably be severed from the records to enable access to the information requested. Based on this finding, we conclude that Manitoba Health had authority to refuse access in full under subsection 17(1) and clause 17(2)(a) of FIPPA, in consideration that the information contained in the records is personal health information, the disclosure of which would constitute unreasonable invasion of third parties' privacy.

SUMMARY OF FINDINGS

1. We found that the requested information is not normally available to the public through existing procedures for access.

2. We found that the information in question is personal health information that is required to be withheld under subsection 17(1) and clause 17(2)(a) of FIPPA, as its disclosure would constitute an unreasonable invasion of third parties' privacy.

3. We found that the personal health information cannot reasonably be severed to provide access in part to any residual information.

CONCLUSION

Our office recognizes that data sharing is vital to health-care research. We also recognize that personal health information of third parties is highly sensitive information that must be carefully protected, in accordance with FIPPA and PHIA.

For these reasons, provisions exist under PHIA and processes are in place through HIPC and within CIHI for the disclosure of personal health information, to ensure that adequate safeguards are in place to protect personal health information, a level of protection that cannot be achieved by an unconditional release of severed information under FIPPA.

Based on the ombudsman's findings, the complaint is not supported.

In accordance with subsection 67(3) of *The Freedom of Information and Protection of Privacy Act*, the complainant may file an appeal of Manitoba Health's decision to refuse access to the Court of Queen's Bench within 30 days following the receipt of this report.

October 28, 2013
Manitoba Ombudsman