Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

REPORT OF THE COMMISSIONER'S FINDINGS

Right to Information and Protection of Privacy Act

Complaint Matter: 2013-1432-AP-744

Date: April 30, 2015

"*Case about access to information found in the Discharge Abstract Database held by the Department of Health*"

INTRODUCTION and BACKGROUND

1. The present Report of the Commissioner's Findings is made pursuant to subsection 73(1) of the *Right to Information and Protection of Privacy Act*, S.N.B. c.R-10.6 ("the *Act*"). This Report stems from a Complaint filed with this Office in which the Applicant requested that the Commissioner carry out an investigation into this matter.

2. The Applicant made an access to information request under the *Act* on April 22, 2013 to the Department of Health (the "Department") seeking:

> "All records pertaining to the Discharge Abstract Database and the National Ambulatory Care Reporting System for acute care hospitals in New Brunswick submitted to the health ministry and/or the health minister and/or New Brunswick hospital 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 the records should be removed."
>
> (the "Request")

3. The Department responded on May 2, 2013 refusing access in full for the following reasons:

> The records we receive from the Canadian Institute for Health Information pertaining to the Discharge Abstract Database and the National Ambulatory Care Reporting System for acute care hospitals in New Brunswick is considered to be personal health data regulated under the *Personal Health Information Privacy and Access Act* (PHIPAA). The *Personal Health Information Privacy and Access Act* supersedes the *Right to Information and Protection of Privacy Act* with respect to personal health information. As such, these records cannot be disclosed except as permitted by PHIPAA.
>
> Record level data is only disclosed outside the health care system for research purposes. This would involve a specific research question that has been reviewed by an ethics committee (established in accordance with the Tri Council Policy Statement). Such requests undergo careful review and require the establishment of parameters for the safe and appropriate transmission, use and ultimate destruction of the information as formalized under a Data Sharing Agreement. If you should wish to undertake this process, please advise and our application form will be provided to you.

> You may wish to have a review of this response under the *Right to Information and Protection of Privacy Act*. You may do so by filing a complaint with the Access to Information and Privacy Commissioner per subparagraph 67(1)(a)(i) within 60 days of receiving this response, or by referring the matter to a judge of the Court of Queen's Bench per paragraph 65(1)(a) within 30 days of receiving this response. Relevant forms are attached.
>
> (the "Response")

4. Not being satisfied with that answer, the Applicant filed a complaint with our Office on June 26, 2013 and remarked that the Request had been refused on the basis that the information requested was considered personal health data. The Applicant restated an awareness of the need to protect personal privacy and the reason why she had specifically requested anonymized information.

5. The Applicant asked the Commissioner to investigate the question of the Department releasing de-identified personal information.

INFORMAL RESOLUTION PROCESS

6. As in all complaint investigations, our Office first seeks to resolve the matter informally to the satisfaction of both parties and in accordance with the rights and obligations set out in the *Act*. For all intents and purposes, in both the informal resolution process and the formal investigation, the Commissioner's work remains the same: assessing the merits of the complaint and achieving a resolution that is in accordance with the *Act*.

7. When the complaint cannot be informally resolved, the Commissioner concludes her work with a formal investigation and publishes her Report of Findings.

8. All steps normally undertaken during an investigation were followed in this matter, including meeting with the Department's officials and obtaining facts about how the Request was processed. Our work included a review of records in determining whether all relevant information had been properly identified and whether access rights had been respected in conformity with the *Act*.

9. We shared our views and findings with the Department, and likewise, we had the benefit of good input from the Department and reasons why the requested information had been refused. The issue of whether the Request may not have been made under the proper statute was determined and that finding was shared with the Department. We explain that point later in this Report.

10. After considerable deliberations, we invited the Department to consider our recommended course of action to provide the Applicant de-identified data and to do so as a means to resolve this Complaint. Despite a good faith effort on the part of the Department, we found that officials were simply not prepared to release the de-identified data on the belief that it could still lead to the identification of individuals and therefore was prevented from doing so under the corresponding protection of health care data: the *Personal Health Information Privacy and Access Act*.

11. The Department did not feel that redactions to the Database would be sufficient to properly de-identify the information. The Department believed it was reasonably foreseeable that the Applicant could cross-reference the remaining Database information with other available information to identify the patients, relying on an objective test in making this argument.

12. We conducted additional analyses of the Department's concerns but regrettably, we could not accept the Department's view. We set out to find answers for all concerned on this most interesting and important question.

13. We therefore advised the Department and concluded our investigation to proceed with the present Report of Findings that addresses the errors in the processing of the Request; more importantly, we provide our legal analysis showing that truly de-identified health care data can be disclosed.

INVESTIGATION

Adequacy of search of records

14. When we reviewed the relevant records, we were informed that the only information the Department had in its possession relevant to the Request was the Discharge Abstract Database; the Department did not have records pertaining to the National Ambulatory Care Reporting System because New Brunswick hospitals do not have "acute care" designations.

15. We reviewed a sample of the Discharge Abstract Database. The majority of the information contained in the Discharge Abstract Database is in the form of raw data submitted by the two Regional Health Authorities in this Province.

16. That raw data is provided to the Canadian Institute for Health Information where that Institute adds additional information for the purpose of statistical analysis. Thereafter, the modified data generated by the Canadian Institute for Health Information is returned to the Department that uses both forms of data (raw and modified) as an information source for the preparation of a wide variety of purposes: both internal management and external reporting requirements, as well as for approved research and internal analytical purposes.

17. Having reviewed a sample of the Database and having received the above explications as to how and why the Department collects this data and records it, we are satisfied that the Department conducted an adequate search to identify all of the records relevant to the Request in this case.

Duty to assist not met

18. The duty to assist provision creates a positive obligation on the public body to offer assistance to applicants in order to ensure that they receive timely, appropriate, and relevant responses to their requests for information, as per section 9 of the *Act*. In our view, the discharge of this duty to assist applies throughout the request process up to and including the issuance of a response to applicants, which connects well with the principle that the response should be helpful and thoroughly answer the applicants' requests.

19. The benefits of doing so are twofold: first, it allows the public body and the applicant to work collaboratively in having the request processed and a response provided on time; second, it will permit the ensuing discussion between the parties to ascertain specific subject areas of information sought (perhaps with a view to narrowing the scope of a large request) or even reach agreement on the issuance of partial responses during a period of time in cases of large requests.

20. In the present case, the Department did not engage in any communication with the Applicant prior to issuing its Response, despite having concerns that the Request was not made pursuant to correct legislation.

21. The Department believed it did not need to communicate with the Applicant because the Department knew what type of information the Applicant was looking for.

22. We find that the Department should nevertheless have communicated with the Applicant to share its concerns and inform the Applicant that the information requested, in the Department's view, could not be released as per the *Personal Health Information Privacy and Access Act*. This would have resulted in discussions that would have been mutually beneficial, while informing the Applicant that the Department in this Province did not have all of the requested information. The duty to assist required the Department to assist the Applicant in this fashion so that the Applicant received a meaningful response, but the Department failed to do so in this case.

Meaningfulness of the Department's Response

23. The Department refused access in full to the requested information based on two reasons:

a) that the requested information was considered to be personal health data regulated under the *Personal Health Information Privacy and Access Act*, which supersedes the *Right to Information and Protection of Privacy Act* with respect to personal health information – leading to requested records processed only under the *Personal Health Information Privacy and Access Act*; and

b) that the requested information consisted of "record level data" that could only be disclosed outside of the health care system for research purposes (as stipulated by subsection 43(1) of the *Personal Health Information Privacy and Access Act*).

24. The Department simply informed the Applicant that the information was refused as requested, that the Request was not made under the correct statute, and the Applicant could undertake a research project process to seek access that way. Although the Response referred to the requested information, i.e. the Discharge Abstract Database and the National Ambulatory Care Reporting System, the Department fell short of informing the Applicant that the Department did not have any records pertaining to the National Ambulatory Care Reporting System.

25. First, we find that the Applicant was not requesting personal health information; the Applicant sought data with the removal of individual personal identifiers. Once personal identifiers have been removed from the Database, the remaining requested data is no longer considered *personal* health information and we find that the *Personal Health Information Privacy and Access Act* does not apply to such information. Accordingly, the

Applicant made the Request properly under the *Right to Information and Protection of Privacy Act* for the reason that the requested information is information relating to the public business of a public body, the Department, being information relating to hospital admissions and discharges compiled by the Department.

26. When a request for access is made under the *Right to Information and Protection of Privacy Act*, the public body, such as the Department, is obligated to answer the request pursuant to the rules of that statute. The relevant records in this case represent data of hospital admissions and discharges compiled by the Department as part of its on-going operations. In this matter, the Department was obligated to issue a response that was in conformity with the requirements found at subsection 14(1) of that *Act* and to rely on that statute to determine whether the Applicant was entitled to receive access to the requested information. In other words, the Department could only refuse access to the requested information by relying on the exceptions to disclosure provisions found in the *Right to Information and Protection of Privacy Act*.

27. The response must not only identify the relevant records and name the specific exception to disclosure relied upon if access to any of the requested information is being refused, but must also provide a brief explanation as to why the specified exception applies. Setting out a response in this manner assists an applicant in better understanding what information is being withheld and why.

28. Although the Request in this case was neither complex nor ambiguous, given the dual role of the Department as a public body and a custodian, and its respect for both applicable statutes, we can certainly appreciate that the Department found itself in an unfamiliar situation in having to respond to an access to information request for health care data that the Department has a duty to protect.

29. The Department met some of the requirements of a proper response by referencing the requested records and explaining the reasons why access was being refused in full; however, we find that in doing so, the Department did not rely on the proper exceptions to disclosure provisions to refuse access and this was due in large part because the Department relied solely upon the rules found in the *Personal Health Information Privacy and Access Act*.

30. In addition, as stated earlier, the Department fell short of explaining to the Applicant that there existed no records relevant to the National Ambulatory Care Reporting System in New Brunswick.

Request for access to health care data

31. When it had to respond to the Applicant's access Request, the Department believed that because the information in the Database consisted entirely of personal health information, the *Personal Health Information Privacy and Access Act* superseded the *Right to Information and Protection of Privacy Act*. The Department held this view given its dual role as both a public body and a custodian and because of subsection 6(1) of the *Personal Health Information Privacy and Access Act:*

> 6(1) The *Right to Information and Protection of Privacy Act* does not apply to personal health information in the custody or under the control of a custodian unless this Act specifies otherwise.

32. We do not agree with that proposition, as in this case, the Applicant did not request access to the Database as a whole and requesting access to personal health information need not be made in all cases under the *Personal Health Information Privacy and Access Act*. We explain.

33. While subsection 6(1) clearly defines the ambit of the *Personal Health Information Privacy and Access Act* as the authoritative statute in dealing with personal health information matters, one must also keep in mind that the statute grants individuals access to their own personal health information. In other words, the *Personal Health Information Privacy and Access Act* does not allow individuals to make access requests to obtain health care information that does not belong to them (unless in special limited cases, such as with an expressly worded power of attorney).

34. As a result, subsection 6(2) of the *Personal Health Information Privacy and Access Act* has already anticipated instances where a custodian, who is also a public body (such as the Department in this matter), receives a request for access to what may be other individual's personal health information and has stipulated that in those cases, the custodian/public body must treat and process the request as if it had been made under the *Right to Information and Protection of Privacy Act*:

> 6(2) If a request in made pursuant to section 7 that contains information to which the *Right to Information and Protection of Privacy Act* applies, the part of the request that relates to that information is deemed to be a request under section 8 of the *Right to Information and Protection of Privacy Act*, and the *Right to Information and Protection of Privacy Act* applies to that part of the request as if it had been made under section 8 of that *Act*.
>
> [Our emphasis]

35. The underlying reason is to direct the custodian/public body to those rules found in Part 2 of the *Right to Information and Protection of Privacy Act* that govern requests and responses, which provide all the necessary rules regarding disclosure – or protection— of personal information belonging to individuals who are not the requester. Moreover, personal information is defined in this *Act* to include *personal health information*.

36. As such, access rights to any information found in government records (such as those held by the Department of Health) are maintained by ensuring that the *Right to Information and Protection of Privacy Act* reigns over the processing of access to information requests, despite the request being for personal information or personal health information.

37. Likewise, even if the Applicant had made the Request under the *Personal Health Information Privacy and Access Act*, subsection 6(2) would have directed the Department, as a custodian and public body, to consider it as having been made pursuant to the *Right to Information and Protection of Privacy Act* because the Request was for data compiled in records held by Department consisting of other individuals' personal health information, and not that of the Applicant's.

38. We also point out that the Applicant did not make an access request for access to the Database as a whole, i.e., the Applicant did not request that the Department disclose the Database with all patients' personal identifiers intact. Instead, the Applicant indicated to the Department of being "*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*."

39. This is an important element of this case; in our view this should have directed the Department to process the Request pursuant to the *Right to Information and Protection of Privacy Act* and not under the *Personal Health Information Privacy and Access Act.* Therefore, the Department should have relied on the provisions of the *Right to Information and Protection of Privacy Act* in responding to the Request and ought to have determined whether access to the requested data was permissible as per those rules, including section 21 protection of third party personal information.

40. Also, the Department believed it could not disclose the information to the Applicant because it was identifiable health care data and that it could not be disclosed outside of an approved research project, and this is why the Department directed the Applicant to present a research project under the *Personal Health Information Privacy and Access*

Act. This is not a proper response to a request made under *Right to Information and Protection of Privacy Act.* The Department had to directly address the Request itself.

41. As a result, we find that the Department's Response to the Request was not in conformity with the requirements of a proper response pursuant to subsection 14(1) of the *Act*.

LAW AND ANALYSIS ON ACCESS TO REQUESTED INFORMATION

42. We agreed with the Department that the Database information, as is, was considered personal health information and therefore ought not to be disclosed to the Applicant in its integral form. In New Brunswick, however, the *Personal Health Information Privacy and Access Act* does not apply to personal health information that has been de-identified. Moreover, the Applicant did not seek identifiable health care data.

43. Again, the Department could not rely on the *Personal Health Information Privacy and Access Act* to refuse to grant access to Database as we explain further below, when the data has been scrubbed of identifiers:

> 3(1) This Act applies
>
> (a) to personal health information that is collected, used or disclosed by a custodian or that is in the custody or control of a custodian, and
>
> (b) to personal health information that was collected before the coming into force of this Act and that is prescribed by regulation.
>
> 3(2) Unless otherwise specifically provided in the Act, this Act does not apply to
>
> (a) anonymous or statistical information that does not, either by itself or when combined with other information available to the holder of the information, permit individuals to be identified.

44. Before we go on to make that determination, however, we need to ascertain what is meant by "identifiers" in the Database, and whether removing identifiers from the Database would still provide access to otherwise protected information.

The Discharge Abstract Database

45. The Discharge Abstract Database (the "Database") consists of a spreadsheet, broken down by reporting years in all manner of information relating to hospital admissions and discharges in general. The Database is not limited to information about a patient's

admission and discharge, but also includes health care number, postal code, date of birth, gender, date and time, institution type, type of admittance, discharge date and time with disposition of patient at discharge, diagnosis, interventions, medical and research audit information, mental health information (source of referrals, method of admission, number of ECT treatments), patients' education, employment and financial status, and so on. As we understand it, the Database can have as many as 900 fields of information. For a single patient, not every field would be filled with data, as that would only apply to those fields that were relevant to the patient's visit.

46. As we can well imagine, the Database thus contains a huge amount of data. In fact, if the Department were to print the requested data for the scope of the Request, being one reporting year, it would represent approximately 224,000 legal-sized pages of information. Additionally, the data contained in the Database is in an encrypted or coded format, which means that to decipher the data, a person needs the data codes and the codes book.

47. We were informed that these code books are accessible to the general public.

48. As a visual reference, this is what a (fictitious) sample of the Database looks like:

3444420150203085B155584625493518762 - 123456789NB01 etc.

49. As we can see, most of the data is undecipherable. With the help of the Master File Layout manual (a code book), however, we can decipher the above data when it is broken down. Each field is defined by the start byte (position of the character) and # of the bytes (the length of the numerical characters), with each field alternative between bold and regular text as follows:

Field#	Field Name	Start byte	# of bytes	Values	Field Description
1	Province	1	1	0-9, N, V, Y, I	0=Newfoundland 1=Prince Edward Island 2=Nova Scotia 3=New Brunswick 4=Quebec 5=Ontario 6=Manitoba 7=Saskatchewan 8=Alberta 9=British Columbia

					N=Northwest Territories V=Nunavut Territory Y=Yukon Territory I=International
2	Institution number	2	4		Facility Identification Number
3	Fiscal Year	6	4	YYYY	Fiscal year of the Discharge
(…)					
12	Health care number	56	12		(Health care number)
16	Postal Code	89	6		Postal Area Designation used by Canada Post (…)

50. Therefore, the first numerical character in the example represents a jurisdiction, with the value 3 representing New Brunswick. The second set of numerical characters, being four characters long, represents the Institution number, and so forth. In the sample above, 4444 would mean Clinic ABC.

51. Having the Master File Layout For would also permit someone to find out a patient's health care number, which is the number that starts at the 56th character in the sequence (and can have up to 12 characters depending on the jurisdiction), and in the sample above, this would be the number 123456789 for that patient.

52. We can therefore state that if a person has access to the Database and the codes, and none of the data has been scrubbed of identifiers, that person could readily decipher a patient's health care or Medicare number, date of birth, gender, and postal code and health care history, which includes tests, interventions, etc. That is why the data cannot be disclosed unless it has been scrubbed and access must be restricted to de-identified information only.

53. Which brings us to this question: can access to health care data take place when it is de-identified?

What is personal health information?

54. "Personal health information" is defined in the *Personal Health Information Privacy and Access Act* to mean identifying information about an individual, in oral or recorded form, if the information relates to, i.e., an individual's physical or mental health, family history or health care history, including genetic information about the individual; the individual's registration information, including the individual's Medicare number; to the provision of health care to the individual, etc.

55. "Identifying information" is further defined in the *Personal Health Information Privacy and Access Act*:

> "identifying information" means information that identifies an individual or for which it is reasonable foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

56. "Registration information" is defined to mean:

> any information about an individual that is collected for the purpose of registering the individual for the provision of health care, and includes a health care number, hospital record number and any other identifier assigned to an individual.

57. In light of the above, we agree that the Database, as a whole, with a person's access to code books such as the Master File Layout, can qualify as individuals' personal health information as defined above. The Database may contain Medicare numbers, dates of birth, age, gender, address, and health care history of an individual that permits the person to identify that individual—that may permit the identification of that individual.

What is truly meant by identifying information?

58. We have been fortunate in obtaining more in-depth knowledge on this very topic through materials and presentations given by the International Association of Privacy Professionals. In particular, we were apprised of techniques used to efficiently anonymize personal data.

59. First, we looked to the term "personal data" used to mean any information relating to an identified or identifiable natural person (the "data subject"). The data subject is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

60. There is a concept of identification referred to as the "ability to single out an individual."

61. In short, that concept means that where the controller of the data, or another person such as the recipient of the data, has a reasonable ability to identify an individual or has the means to single out an individual, this means it is *identifying information*.

Can identifying information be de-identified?

62. This brought us to consider whether identifying data could be de-identified.

63. We examined an important method used known as the *Safe Harbour* method. It emanates from the United States and is a method used to de-identify personal health information in accordance with the Privacy Rule found in the American *Health Insurance Portability and Accountability Act* ("HIPPA") that is founded on an objective evaluation. That legislation is similar to our *Personal Health Information Privacy and Access Act*. The HIPPA Privacy Rule, when applied, allows the controller of the data to use and disclose information that does not identify and does not allow the means to identify an individual. This Rule further stipulates, on an objective basis, that the controller of the data has no reasonable basis to believe it can be used to identify an individual.

64. In summary, the de-identification standard stipulates that health information is not individually identifiable if it does not identify an individual and if the data controller has no reasonable basis to believe that it can be used to identify and individual.

65. In order for the *Safe Harbour* method to be used effectively, the following requirements must be met:

> (i) that the individuals' identifiers or of relatives, employers or household members of the individual must be removed from the dataset:
>
> a) Names
> b) All geographic subdivisions, smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
> i. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
> ii. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people are changed to 000.
> c) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, date of tests, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
> d) Telephone numbers
> e) Fax numbers
> f) Email addresses
> g) Social security numbers
> h) Medical record numbers

i) Health plan beneficiary numbers
j) Account numbers
k) Certificate/license numbers
l) Vehicle identifiers and serial numbers including license plate numbers
m) Device identifiers and serial numbers
n) Web universal resource locators (URLs)
o) Internet Protocol (IP) addresses
p) Biometric identifiers, including finger and voice prints
q) Full-face photographs and any comparable images
r) Any other unique identifying number, characteristic, or code, except as permitted by section "Re-identification"; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(Source: from the US Department of Health and Human Services at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html)

66. As we can see, when this method is used and personal health information is de-identified, the data is no longer considered protected by the HIPPA Privacy Rule because de-identified data no longer falls within the HIPPA definition of protected health information.

67. According to our research, the mere hypothetical possibility of singling out an individual is not enough to consider the person as "identifiable". It is also a requirement that there be tangible evidence to show that re-identification is plausible.

68. Based on this analysis, we therefore agreed with the Department that the test to determine whether information falls within the definition of "identifying information" is an objective one: whether it is likely reasonable that a recipient of the data *could*, in the circumstances at hand, and by using the relevant information with any other information available to him or her, identify the individuals to whom the relevant information relates.

69. The Department was also correct in saying that in the event that the Database information (with identifiers removed) could still allow for the identification or could still single out individuals, in this case by the Applicant, this would mean that neither the *Right to Information and Protection of Privacy* or the *Personal Health Information Privacy and Access Act* would permit its disclosure, except in controlled limited circumstances such as approved research projects.

70. A key factor remained, however, as to whether the data controller (the Department) had reasonable basis to believe that the de-identified information of the Database could lead to the identity of individuals.

71. In other words, the Department still had to show – not just speculate - that the Applicant had the ability or means to single out or identify the individuals from the Database, as de-identified, so as to be entitled under the *Act* to properly refuse access with reasonable fact or argument.

In this case, could the information in the Database be truly de-identified?

72. With the objective test in mind, we set out to consider redactions to the Database, such as removing the patients' Medicare numbers, dates of birth, gender and postal codes, to determine its level of anonymity. We found this was not sufficient given that it was reasonably foreseeable that the remaining data could be identifiable, should the Applicant have access to other information, including the code books (the Master File Layout). For instance, with the help of the Master File Layout, it would be reasonable to foresee that the Applicant might be able to identify individuals by looking at their chart numbers, institution numbers associated with every visit to a particular hospital.

73. We therefore suggested applying the *Safe Harbour* method described above. This meant that additional identifiers would be redacted from the Database as they qualified as personal health information identifiers that warrant protection from disclosure to the Applicant:

- institution numbers
- chart numbers
- register numbers
- residence codes
- all dates, except year of birth dates
- admission dates
- discharge dates
- test dates, start and end dates,
- age codes,
- age units, and
- age groups.

74. We found this approach to be the correct, reasonable and safe manner in which to de-identify the requested data in this case. The Department, however, maintained its position that despite removing identifiers such as those above, it believed there still existed a risk of re-identification of the individuals. The Department, in our view, was still unable to supply reasonable fact or argument as to why this concern was foreseeable in the circumstances of this case.

75. In other words, the Department could not meet the test to show that the Database, once scrubbed of personal identifiers, could be used by the Applicant, either alone or with other information, to re-identify individuals. Nevertheless, we set out to determine whether there indeed existed a risk of re-identification.

76. When disclosure of de-identified data is being contemplated, such that personal information is no longer considered "personal data", we rely on the industry standard of the acceptable level of risk: that re-identification is not likely reasonable to occur. "Not likely reasonable" is linked to a level of reasonableness or acceptable level of risk when assessing the possibility of releasing the data. Factors include the amount of effort, time, money, and technology that would have to be spent to re-identify the individual who is the subject of the data.

77. We accept the industry standard that once the data is no longer identifiable and it is not likely reasonable that the recipient of the data could use it for re-identification purposes, it should therefore be considered an acceptable risk to release such de-identified data.

78. In this case, in applying such standard, we still cannot find any fact or argument and it is not likely reasonable that the Applicant could use the data to re-identify the individuals.

79. Therefore, with the removal of the identifiers described above (using the Safe Harbour method), we find there is an acceptable level of risk to permit the Department to grant access to the Applicant the Database information with the stipulated identifiers removed. The Department would first anonymize the original data so that it is no longer considered "personal data" and then would be able to share it with the Applicant as the threshold of the acceptable risk would be met in this case.

Disclosure of Database information under the *Right to Information and Protection of Privacy Act*

80. Having found that the Request was properly made under the *Right to Information and Protection of Privacy Act*, we must now determine whether the requested information can be disclosed as per the rules stipulated in the *Act* relating to an access request or whether it must remain protected. Under the *Right to Information and Protection of Privacy Act*, "personal information" is defined to mean "recorded information about an identifiable individual".

81. As a starting point, personal information belonging to third parties cannot be disclosed where doing so would be an unreasonable invasion of their privacy (section 21), unless consent is obtained, or disclosure without consent is permitted. Neither of these instances applies in this case.

82. We know that the Database as a whole contained personal health information of individuals (hospital visits, health history, registration information, etc.) and information that could be deciphered with the help of code books, such as the Master File Layout to permit identification. Disclosing the Database in its integral format, without consent of all those to whom the information relates, or without a permitted instance without consent, would be an unreasonable invasion of those individuals' privacy, and thus, contrary to section 21.

83. With stipulated personal identifiers removed from the Database, however, we find that the remaining information would only consist of health information but not "personal data" as there is neither no tangible evidence nor reasonable likelihood that the Applicant would be able to re-identify the data.

84. We again point out that the Request was for records of the Database minus any personal information about patients, including any personal identifiers.

85. Given our earlier findings, the Database could be scrubbed of individuals' personal identifiers by removing the following information for each patient:

- Medicare or health care numbers
- Gender
- Date of birth
- Age
- Postal code
- institution numbers
- chart numbers
- register numbers
- residence codes
- all dates, except year of birth dates
- admission dates, discharge dates
- test dates, start and end dates,
- age codes,
- age units, and age groups.

86. We find that the Department could have removed these identifiers from the Database and then considered whether the remaining data found in the Database could be disclosed. As per our analysis above, the remaining data would be truly de-identified.

87. As de-identified data, and with no likely reasonable risk of re-identification, we find there is no concern of risk or harm to privacy, and it follows that there is no exception to

disclosure in the *Act* that prevents the remaining Database information from disclosure on the basis of an unreasonable invasion of privacy (under section 21).

CONCLUSION AND RECOMMENDATION

88. Based on the above, we find that the Applicant filed the Request under the correct statute, being the *Right to Information and Protection of Privacy Act*, and that the Department ought to have processed the Request under that statute.

89. The Applicant did not seek access to personal identifiers found in the requested Database. The industry standards, including the Safe Harbour method for de-identification, provide a prudent method to de-identify personal health information to permit its safe and lawful disclosure and the Department could have utilized these standards to assist the Applicant in this case and to provide access to de-identified health care data.

90. In applying these standards, and by removing from the Database the individuals' Medicare number, date of birth, gender and postal code, institution numbers, chart numbers, register numbers, residence codes, all dates, except year of birth dates, admission and discharge dates, test start and end dates, age codes, age units, and age groups, the Database can be scrubbed of identifiers to render the information truly de-identified and as a result, subject to disclosure without risk of harm to privacy.

91. In light of the above, and pursuant to sub-paragraph 73(1)(a)(i) of the *Act*, the Commissioner therefore recommends that the Department of Health grant access to the Applicant of the Discharge Abstract Database, in part, by first removing from the Database, the following redactions:

> Medicare number, date of birth, gender, postal code, institution numbers, chart numbers, register numbers, residence codes, all dates, except year of birth dates, admission and discharge dates, test start and end dates, age codes, age units, and age groups.

Dated at Fredericton, New Brunswick, this _____ day of April 2015.

_____
Anne E. Bertrand, Q.C.
Commissioner