NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Recommendation 15-140
File: 15-121-4
October 28, 2015

BACKGROUND

This privacy complaint arises out of information received by the Complainant as a result of an Access to Information Request. The Complainant (who shall be referred to herein as A.B. for ease of reference) was concerned about the way in which his personal health information had been used and disclosed in making decisions with respect to his health care.

A.B. had received a diagnosis and treatment from a leading specialist prior to his move to the Northwest Territories. Upon his arrival in the Northwest Territories he sought to continue his treatment in accordance with his previous physician's plan for him. The treatment, however, was not an "insured service" under the NWT's Health Care Plan. As a result of an Access to Information Request, A.B. learned that his physician had disclosed between 10 and 19 pages of his medical file, which included a confidential psychiatric evaluation and the resulting assessment, to a number of individuals within the Department who had no direct role in his health care. The disclosure by his physician and the resulting additional disclosures was not for the purpose of verifying his diagnosis or the treatment plan, but was rather for the purpose of determining whether or not the Department of Health and Social Services would cover the cost of the recommended treatment under the NWT Health Care Plan. A.B. was not asked for his consent to this disclosure, nor did he provide any such consent. In reviewing the records he received as a result of his Access to Information request, he counted approximately 15 people who appear to have had access to these medical records or information about his medical issues without his knowledge or consent. In addition, he notes that it would appear from the records he obtained that there were additional, unknown persons who were participants in meetings in which his situation was discussed who may, or may not, also have had access to the files. In A.B.'s words:

> The issue seems to begin with [the physician] forwarding pages of unaltered confidential medical records to the insured services division of HSS. It is reasonable to assume that [5 named individuals within HSS] have all had access to these files. I am concerned that my private and confidential records were further shared throughout HSS without my consent and without being redacted. I am also concerned that the nature of the decision being made did not warrant access to these particular records yet they were still shared with at least 5 people who did not require them in order to make their decision about whether they would cover [the treatment] as an insured service.

A.B. has requested that any of his medical records which may be stored electronically or in print (email, attachments, meeting notes or other correspondence) other than in his own family doctor's office be removed and destroyed.

THE DEPARTMENT'S SUBMISSIONS

The Department acknowledged that there were two events in which A.B.'s personal health information was disclosed to the Health Services Administration (HSA) Office of Health and Social Services. The first was to obtain approval for funding for the medical treatment recommended and the second was in connection with a request by A.B. for an amendment to his health care registration. The first disclosure was made by A.B.'s physician. Health and Social Services says that the second disclosure was made by A.B. himself.

1. Request for insured service

The Department indicates that when a request for an "uninsured service" is sent to the HSA office, it is initially processed by the Insured Services staff. The information is then sent to the Chief Clinical Advisor for review and recommendations. The Chief Clinical Advisor, "requires all pertinent information" to make an informed clinical decision about whether or not to approve the uninsured service for exception coverage as an insured

service under the Northwest Territories healthcare plan. If the recommendation is to approve the funding, the HSA Director normally authorizes the procedure then the Insured Services staff contacts the client's physician. "All pertinent information that the Chief Clinical Advisor used to make a decision is then sent to the HSA Director". No explanation as to the purpose for this disclosure or why the HSA Director requires such detailed personal health information is provided by the Department, other than a reference to legislation as set out below.

If the recommendation is to decline the request, the HSA Director confirms the denial and the Insured Services staff contacts the client's physician with that information. Once again, "all pertinent information" is sent to the HSA Director. In some instances, the Chief Clinical Advisor will note that the service is covered in other jurisdictions but not in the NWT. In these circumstances, the Chief Clinical Advisor can recommend that the service be covered from a policy perspective. The HSA Director would then discuss the matter with the Assistant Deputy Minister (ADM), Clinical Services, in his capacity as Director, Medical Insurance, to determine if the service should be approved for all future applicants for this treatment.

The Department has referred me to the following Acts and Regulations to support their authority to share personal health information in this manner:

Medical Care Act, Section 5

5. The Director shall, in accordance with this Act and the regulations,
   (a) assess the eligibility for entitlement of persons to insured services;
   (b) assess the amounts payable for insured services; and
   (c) authorize payment of the amounts assessed under paragraph (b) out of the Consolidated Revenue Fund

(i) to the medical practitioner who provided the insured services or to a person on his or her behalf, or
(ii) to the insured person who received the insured services.

Medical Care Regulations, Section 2

2. The Director shall designate a medical practitioner as a medical adviser to review and make recommendations
   (a) in respect of the amounts that should be allowed on claims for benefits; and
   (b) in respect of such other professional matters as may be referred to him or her by the Director.

Medical Care Regulations, Section 6

6. A claim for a procedure that is not listed in the tariff shall be assessed by the Director upon submission and receipt of as much clinical description as is, in the opinion of the Director, practicable under the circumstances.

In this case, the Department says that A.B.'s personal health information was shared with the insured services staff, the HSA Director and the Chief Clinical Advisor to determine if the service would be insured (four people in total).

The Department says that the HSA Director also consulted with his supervisor, the ADM, Corporate Services, from a policy perspective but did not disclose A.B.'s sensitive personal health information to the ADM.

In the second event, the Department says that A.B. sent a request to the HSA office to have his health care card (and therefore his health care registration) information amended. They say that there was no clinical or medical information attached to the request. The request was reviewed by four employees (including two who had been

provided with copies of A.B.'s health records in the first event). In this case, in addition to those directly involved in dealing with the request, it was thought to be a matter that required further consultation from a policy perspective because the change requested might come up again and this decision, therefore, might affect future decisions in similar circumstances. For this reason, the request was shared with the ADM, Corporate Services, and with the Policy Legislation and Communications Division. The Department says that no personal information was disclosed, but A.B.'s request and his situation were. This consultation included, in addition to the ADM, five additional employees in the Department but in a division other than HSA.

It is the Department's position that at no time was A.B.'s personal information shared with staff outside the Health Services Administration Offices.

The Department, in its submissions to this office, agreed to dispose of any copies of the clinical and medical information submitted to the HSA office in support of the request to cover A.B.'s treatment through the health insurance program. They also indicated that A.B. could limit future access to his personal health information by notifying his physician of the restrictions on his "consent".

THE COMPLAINANT'S RESPONSE

A.B. was provided with a copy of the department's submissions and invited to provide any further input he might have. Nothing further was received from the Complainant. In his original correspondence, however, he did provide a number of emails and other records which supported his assertions that his information was distributed among many people within the department. These documents are, as A.B. pointed out, revealing. While the public body says that they did not share A.B.'s personal health information with the ADM or with others involved in the "policy discussion", it is clear from these email chains that this is not accurate. The email correspondence provided by A.B. indicate clearly that the ADM, among others, was included in an email chain in which A.B.'s personal health information was disclosed. The emails contained sensitive

health information which clearly identified A.B. as the individual whose information was being discussed.

DISCUSSION

This complaint arose prior to the coming into effect of the *Health Information Act*. The law in effect at the time of the alleged breaches was the *Access to Information and Protection of Privacy Act*. It is that Act, therefore, that must be applied in this case.

Section 43 of the *ATIPP* Act outlines how personal information in the possession of a public body can be used:

> 43. A public body may use personal information only
>
> (a) for the purpose for which the information was collected or compiled, or for a use consistent with that purpose;
>
> (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use; or
>
> (c) for a purpose for which the information may be disclosed to that public body under Division C of this Part

Section 48 outlines when personal information can be disclosed (i.e. - used outside of the office which collects the information). The relevant parts of that section allow the disclosure of personal information in the following situations:

> 48. A public body may disclose personal information
>
> (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose;
>
> (b) where the individual the information relates to has identified the information and consented, in the prescribed manner, to its disclosure;
>
> ....

(k) to an officer or employee of the public body or to a member of the Executive Council, where the information is necessary for the performance of the duties of the officer or employee or the member of the Executive Council;

The public body does not dispute that significant and extremely sensitive personal health information about A.B.'s situation was disclosed by his physician to the Health Services Administration Division of Health and Social Services. There is nothing before me that suggests that A.B.'s physician discussed with A.B. the fact that he would be doing this prior to the information being disclosed, nor the extent of the information which would be disclosed. While the Department does not say so directly, they appear to assume that the physician had A.B.'s consent to the disclosure of his information for this purpose. A.B. says that he did not consent. We have not heard from the physician.

Addressing firstly whether the physician had the authority under the Act to disclose A.B.'s sensitive medical files, in my view, this disclosure went far beyond any implied consent that A.B. might have given to the sharing of his personal health information. Furthermore, while we are talking about this disclosure as a disclosure under the *Access to Information and Protection of Privacy Act*, my conclusion would be the same under the *Health Information Act*. Consent to disclosure must be knowledgeable consent, which means that the patient must have a clear understanding as to what information will be disclosed and how the information will be used. There may have been some very high level discussion between the patient and the physician about the fact that the physician would have to make a request for this health service to be paid for as an insured service. However, the physician clearly did not tell A.B. what would be disclosed or how many people would have access to this extremely sensitive personal health information. There was no consent to the disclosure.

The question then becomes whether the information was disclosed for a "consistent" purpose. The measure of what is consistent is not defined. Clearly, A.B. did not consider the disclosure of significant portions of his health records, including a psychiatric assessment, to be a disclosure "consistent" with the purpose for which the

information was gathered, which was to obtain a specific medical treatment. In most cases, the consent that can be implied from a patient seeking medical attention is quite limited in scope. There may be an implied understanding between the patient and the physician that some minimal personal health information will be disclosed to a health insurance agency used by the patient to compensate the physician. The case in point, however, is much different. This case involved the disclosure of parts of A.B.'s medical file, including psychiatric reports, to seek approval for the treatment, not a limited disclosure for payment purposes. I am not convinced that this can be considered a "consistent purpose" justifying the disclosure.

Was this disclosure necessary for the Director of HSA to complete his job function? In this case, the Director's job is to determine whether the treatment was an appropriate use of the health insurance system. My concern lies in the extent and the nature of the information disclosed. Did the Director of HSA really need all of A.B.'s detailed medical records to make this decision? If he did, considering the very sensitive nature of the records in question, should there not have been some discussion with A.B. about the process and the fact that his information would have to be shared in order to process the request? In my view, the patient should be made aware of this kind of disclosure and be given the opportunity to retain some control over how much information is being disclosed and to whom. At the very least, he should know that there will be a disclosure.

One of the ten rules of good informational practices is that you collect, use or disclose only the minimum amount of information necessary to accomplish the intended goal. It seems to me that in this case, at the very least the records should have been redacted so as to remove reference to A.B.'s name, community of residence and contact information. Nor is there anything to explain why it was necessary for the Director (or his medical advisor) to have A.B.'s psychiatric records - surely it would be sufficient to provide a summary or an edited version of these records. This is true for all of the medical information disclosed. The decision as to whether or not to cover this treatment was a policy decision - is this the kind of treatment which the health care system in the Northwest Territories should be paying for? - not a medical one. A.B. already had not one but two medical opinions that it was necessary for his health. I am not convinced

that it was truly necessary to disclose so much of A.B.'s medical information to approve payment for the treatment.

I have reviewed some of the emails that were exchanged between the medical advisor and the HSA office. A.B.'s name was used in the "subject" line of the emails. There was information in the body of the emails which referred not only to A.B.'s specific diagnosis, but the name of his psychiatrist. So not only are we talking about A.B.'s actual medical file records, but also the information which was put in the email correspondence.

How does this all relate to the provisions of the *Medical Care Act* and the *Medical Care Regulations* referred to by the public body? Section 5 of the *Medical Care Act* allows for the Director of HSA to assess the "eligibility for entitlement of persons to insured services". This is not what the issue was in this case. There was no issue as to whether A.B. was entitled to receive insured services. The issue was whether or not the treatment requested should be covered. Nor is there any question that the Director of HSA had the authority to seek advice from the medical advisor.

The most relevant provision in this case is Section 6 of the *Medical Care Regulations* which addresses the issue of when there is a claim for a treatment that is NOT listed in the tariff, which is essentially what the circumstances were in this case. This section is not, however, very clear in terms of what kind of information can be collected. It refers to "as much clinical description as is, in the opinion of the Director, practicable". Does the term "clinical description" extend to specific personal health information? In my view, it does not.

With respect to A.B.'s request to change the information on his health care registration, he did, in fact make the request for the change. His email was directed to the Director of HSA and three other individuals. To that email was attached a letter from A.B. which I do not have, but which would have contained at least some basic personal health information about A.B.. The Director of HSA, who was the primary recipient of this correspondence obviously felt that he needed to consult with others on a policy level

about the requested change. Unfortunately, rather than send out a memo on the issue, it appears that the Director merely emailed the entire content of A.B.'s correspondence, which was in turn forwarded several more times. Each time, A.B.'s name and at least some background about his situation was disclosed to individuals who did not need that information for the purpose of making the policy decision in question.

CONCLUSIONS AND RECOMMENDATIONS

In my view, A.B.'s privacy was breached several times in the process of making a decision as to whether or not a treatment which was deemed medically necessary for him was going to be covered by the NWT Health Care system. The physician should never have disclosed the detailed personal information and medical charts to the administrative body making this decision without fully discussing the matter with the patient first. The more sensitive the information, the more care has to be taken in ensuring that it remains confidential and private. If the information disclosed had been no more than a name and address and a report about a broken leg, the disclosure, while still a breach of privacy, would not have been as serious as this one was. The information being exchanged and discussed by means of unencrypted email among several individuals in this case was far more sensitive.

The information shared with the Director's office should have been redacted or summarized so as to protect the identity of the patient before it was given to the Director's office. The request was for a decision on a policy level. It was not a medical decision. There should be no reason for someone making a policy decision to require personally identifiable information to make that policy decision. In fact, Section 28 of the new *Health Information Act*, prohibits the collection of personal health information where non-identifying health information would be adequate for the intended purpose:

> 28.(1) Subject to subsection (3) and the regulations, a health information custodian shall not collect, use or disclose personal health information if non-identifying health information would be adequate for the intended purposes of the collection, use or disclosure.

This case also demonstrates how oblivious and lackadaisical many of us have become about the scope of information we share by email. Quite apart from the first disclosure by the physician, the information was shared and discussed very openly, with A.B.'s name emblazoned in the emails. While the public body says that A.B.'s personal health information was not shared with the Deputy Minister, it clearly was. The content of some of the emails provided by A.B. clearly show his name and other specific information about his health needs within the emails themselves. There is no indication that the emails were encrypted or otherwise protected from going astray. The same holds true for the discussion surrounding A.B.'s request for a correction to the information on his health care card.

This situation arose prior to the coming into effect of the *Health Information Act*. That said, the ten internationally accepted privacy principles, on which the *Access to Information and Protection of Privacy Act* is based, say much the same thing and my conclusions would be the same under either piece of legislation.

As I have noted before, once privacy is breached, there is no taking it back. There is, therefore, little that can be done to fix the breach of privacy in this case. A.B. has, however, asked that the personal health records that were shared be destroyed. The Department has agreed to do that.

1. I **recommend** that the public body physically destroy any copies of A.B.'s personal health records in the offices of the Director of HSA and/or the Deputy Minister's office (including any information contained in email records) and confirm with A.B. when this has been completed.

On a more general and ongoing basis, I make the following recommendations:

2. I **recommend** that before a request is made for coverage for treatment of an "uninsured" service on behalf of a patient, the patient be informed that the request will be made and advised of the kind and scope of his/her personal health information which will be disclosed for that purpose. In such

circumstances, express consent to the disclosure will be required under the new *Health Information Act* and there should, therefore, be a written policy about this.

3. I **recommend** that the Director of HSA establish clear written policies about the nature of the "clinical information" he requires in order to make a policy decision as to whether or not an "uninsured" service will be covered. Such policies should include a restriction on the amount and the nature of personally identifying information required for such decisions, limiting it to information absolutely necessary for making the policy decision. For example, while the Director may need to be able to identify the patient by means of a health care number so that the health service can be approved for that individual, he does not need the individual's name or community or residence and the medical advisor has no need to know the identity of the patient at all. While it may be appropriate to note that the patient has had a psychiatric assessment done, is it necessary for either the Director or the Medical Advisor to have a copy of the assessment or would a summary of the results be sufficient? As the Director does not appear to be a physician, how much information does he actually need when the issue is one that is being referred to the Medical Advisor. The policy should, perhaps, specify that such a request should be made directly to the Medical Advisor or that any medical health information be submitted directly to the Medical Advisor, avoiding the Director and his staff altogether. It is important that this policy be detailed and take into consideration exactly what information is needed to make the policy decision to fund and who actually needs to access the information in order for the decision to be made. This kind of specific policy will be all the more important under the new *Health Information Act.*

4. I **recommend** that all physicians and other medical personnel employed by the Department of Health be reminded, on a continuing and ongoing basis, that the new *Health Information Act* prohibits the disclosure of personal health information when non-identifying information will suffice and, as a corollary to that, where personally identifying information must be used, the amount of such information disclosed should be limited to that which is absolutely necessary.

5. I **recommend** that the Department review their policies with respect to the use of unencrypted email for the purpose of discussing sensitive personal health information and that these policies include when emails containing an individual's personal health information can and cannot be "forwarded" to a third party for any purpose.

Insofar as A.B.'s request that any personal information related to his situation from this point forward be held only by or in the offices of his personal physician, the new *Health Information Act* provides that a patient can limit access to his/her personal health information by providing directions in writing to that effect. I would encourage A.B. to discuss this matter with his physician and put in place such restrictions as he feels are appropriate, keeping in mind the affect that such restrictions might have on his overall health situation.

Elaine Keenan Bengts
Information and Privacy Commissioner