NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 19-HIA13

File: 17- 244 - 6
April 30, 2019
Citation: 2019 NTIPC HIA7

OVERVIEW

The Complainant in this case is an employee of the Northwest Territories Health and Social Services Authority (NTHSSA). He has had ongoing concerns about processes and procedures in place (as well as, in some cases, the absence of processes and procedures) and the resulting threat to the privacy of patient information. He has asked my office to investigate a number of concerns that he has with respect to processes and procedures and practices within HTHSSA.

1. As an employee of the NTHSSA, the Complainant has been provided with access to the electronic medical record (EMR) of patients. The EMR is the tool used by NTHSSA to keep track of clients and their medical information. According to the Complainant, while it is a "roles based" system which limits the amount of information that can be viewed by each employee in accordance with his or her "role" or job description, all employees, regardless of their role, have access to basic "encounter record" information. He says that the encounter record lists all of the reasons a client has accessed an appointment and often also reveals additional sensitive personal health information such as mental health diagnoses, participation in a methadone program; cancer treatment and abortions.

   The Applicant argues that too much information is made available to too many employees. His concerns are exacerbated by the fact that, with the amalgamation of most regional health authorities in the Northwest Territories, and the implementation of the Electronic Medical Record (EMR) the number of people with access to this information has increased dramatically because the

EMR is now available to all employees in all clinics throughout the Northwest Territories. He argues that NTHSSA has an obligation to do a better job of restricting access to sensitive personal health information to only those who "need to know" to provide services to the patient.

2. The Complainant alleges that clinic assistants (usually the first person a patient will have contact with when booking an appointment and when arriving for an appointment) have access to a screen called the "Medical Summary Screen". He says that this screen includes a "problem list" which includes sensitive issues similar to the information outlined above and a list of the medications the patient is on. He argues that clinical assistants do not need this information to do their job.

3. The Complainant says that any health provider can write notes within the EMR for any service provided to clients. He argues that most patients are not aware that there are a significant number of health providers able to access that information if they choose to do so. He alleges that while the Authority has argued that staff who do not need to see these notations "should" not access that information there are no physical or technological safeguards preventing it from happening and no routine auditing done so as to dissuade people from snooping or other inappropriate access. As a result, he says, patients are not aware of who, exactly, has access to their personal health information or how easy it is to gain such access.

According to the Complainant, auditing is only done in 2 situations:

a) when a client makes a formal request for an audit of who has accessed his/her records (and most people don't know they have the right to make such a request);
b) when a staff person with the same last name as the name of a patient accesses the file, the transaction is flagged and in some cases an audit will be run.

4. The Complainant feels that he should be able to look up his own personal health information but notes that if he does it will be flagged and he will likely be punished for doing so. He argues that this seems ironic when every other employee of NTHSSA can easily access this information with little chance of being detected/punished.

5. With all health information throughout the system providers having access to the EMR, the Complainant argues that there are very different ideas about who *should* have access to what information. More and more, he says, he hears the argument from the NTHSSA that anyone within the "circle of care" is entitled to access to any client file, at least to the extent that their role allows. He notes:

> A physician, a home care worker, a nurse practitioner, a counsellor, a public health nurse, a psychiatrist, a dietician etc (*any* health care provider from *any* of the NWT communities who have access to the EMR) may very well think they should have access if say, they believe "it is the best interest" of the client. Of course, the client will not be part of defining what that interest is.

6. The Complainant maintains that the current EMR does not have the ability to "mask" - that is the ability to hide certain personal health information from specific EMR users and that patients are not, therefore, able to exercise their rights to control who has access to their personal health information as provided for in the *Health Information Act.* Furthermore, he says, patients are not told that they have the right to put such limitations on their health records.

7. The Complainant alleges that notes from the psychiatric nurses and psychiatrists with the out-patient program are stored on the EMR. These notes frequently contain detailed sensitive information and, he says, clients in the program are not aware that their notes are being stored in this "unprotected" way. The Complainant states that *all* service provider staff have access to such notes and that given the continued emphasis on collaboration and circle of care he is

concerned that many service providers will see no issue in accessing these notes without client permission if they are working with the client in some other capacity.

8. The Complainant says that while counselors no longer save their notes on the EMR, they continue to "complete" their sessions in the EMR under the Encounter Record and, when they do so, they are unable to avoid seeing personal and sensitive health information that the client may or may not be ready to disclose and which counseling staff do not necessarily need to know. Further, he says, the client will be unaware that the counselor has access to or has seen the information on the encounter record.

9. The Complainant states that when physicians make a referral to the Community Mental Health and Adult Services (CMHAS) for a patient to receive counseling or out-patient psychiatry, they use the same form as they use if they were making a referral to a medical specialist - that is, they include a list of the patient's medical diagnoses past and present. It is his position that this information is not required for the client to receive counseling or psychiatric services. To illustrate the reason that this is inappropriate, he provided the following scenerio:

> A psychiatrist who assessed a patient sends a note to the counselor working with that patient suggesting that the counselor should explore with the patient the impact that a previous [medical issue] might be having on the patient's mental health. The patient has not informed the psychiatrist about the [medical issue]. The patient has not mentioned the [medical issue] during the intake process for counseling, nor has the issue been raised by the patient during several counseling sessions. The information provided by the psychiatrist is from the patient's EMR and the patient is unaware that the psychiatrist had accessed this information or that he has disclosed it to the counselor. Should the patient find out about this, there is a high likelihood that [he/she]

will lose trust in [his/her] physician, [his/her] psychiatrist and [his/her] counselor and [he/she] may choose, as a result, to avoid all three and not get the help that [he/she] needs.

10. As an employee with the NTHSSA, the Complainant says he has not been given a clear understanding of what the term “implied consent” means.

11. The Complainant alleges that personal health information, including counseling and psychiatric patient information, is “commonly” sent and received through unencrypted email. The Complainant has received misdirected emails with a client’s personal health information but, when this has been reported he has been told that this does not constitute a breach because it was sent and received within the NTHSSA.

12. The Complainant says that there has been a practice among some counseling staff of sharing client information with other medical practitioners without clear consent.

THE CUSTODIAN’S RESPONSE

In order to assist me in understanding how the EMR works, I asked for a detailed description from the NTHSSA. They advised that the EMR is a single electronic medical record for all outpatient clinical charting in the Northwest Territories which allows for an efficient and effective means of retaining and communicating important and relevant health information for all residents of the Northwest Territories using out-patient services. They say that “this results in the right providers having the right information, at the right place, and at the right time,” leading to better clinical outcomes and HSS system sustainability. As of March, 2018, the NWT EMR has been deployed to authorized users in all NWT communities with local health facilities.

Approved end users can connect to the EMR from their work stations and some are also able connect to the EMR remotely from a mobile workstation, such as a

Government issued laptop from anywhere using a Virtual Private Network connection (VPN).

Access to the EMR is granted “for authorized purposes only”. Access to personal information is determined “according to the user’s business function” as prescribed by the Territorial Roles Based Access Classification (RBAC). This classification system is the standard model used in most Canadian jurisdictions and is considered a “best practice”. The classifications and the access required for each role in the system is revised over time to “reflect the changes in health and social services system environment, and the implementation goals of the territorial EMR project.”

Access to the system is granted only to authorized individuals “where there is a need for access to information and to the functionality provided by the application”.

NTHSSA points out that the EMR used in the Northwest Territories is a system “approved by Canada Health Infoway”, an organization tasked with facilitating the adoption of electronic solutions to health information management throughout the country. Canada Health Infoway has “demonstrated by way of a prescribed process that EMR is a ‘trusted solution’ and conforms to both national and international privacy, security and interoperability standards.”

NTHSSA advised that, although auditing in the past was limited as outlined in the Complainant’s letter, regular auditing was instituted with the “go-live” of the full Northwest Territories EMR. They indicate that there are a range of auditing tools within the EMR to verify access. Improvement of privacy and security is continually addressed with “ongoing management of physical, administrative and technical safeguards”. In addition to monitoring use, audits are used to inform on needed adjustments to the role based access and to amend and revise training materials for employees.

The NTHSSA advises that the amalgamation of previous independent authorities under one authority has not changed “the principles by which PHI [personal health information] is collected, used and disclosed across the system”. Policies and

procedures are largely the same, though there is a plan to do a broad review of policy and procedures. The new organizational structure has also added significantly to the resources available to manage quality, privacy and risk across the system with the addition of staff dedicated specifically to quality of service, best practices, risk management, client experience, privacy and policy development.

DISCUSSION

The Complainant has raised a number of legitimate concerns about patient privacy within the system. This is not the first time he has raised these issues. He raised many of the same or very similar concerns in 2011 prior to the coming into effect of the *Health Information Act* and the amalgamation of all but two of the regional health authorities then in place throughout the Northwest Territories. At that time, I produced Review Report 12-104 in which many of these same issues are discussed in the context of the system as it existed at the time. The landscape has changed significantly since then, most particularly with the coming into force of the *Health Information Act.* That said, many things have not changed, including the tool used for electronic charting. Some of the discussion in that report, therefore, is relevant here.

As noted in my previous report, electronic medical records are the way of the future and will address many of the more difficult and complex issues surrounding the effective and efficient use of health care resources:

> In November of 2002, Commissioner Roy J. Romanow released the final report of The Commission on the Future of Health Care in Canada, entitled “Building on Values, The Future of Health Care in Canada”. In it, he pointed out the many, many benefits of EMRs, from improved diagnoses, treatments and results, to the minimization of errors and far greater efficiency. However, EMRs also raise a number of real and very difficult privacy issues and Mr. Romanow’s report recognized that as an important part of the solution. He stated:

> There are clear benefits to Canadians from electronic health records. They would have access not only to their own health information but also to a comprehensive base of trusted and reliable information about a variety of health-related issues. Canada Health Infoway should take the lead in promoting harmonized privacy rules across the country, and breaches of privacy should be treated as an offense under the Criminal Code of Canada.

This theme was repeated in a more recent paper co-authored by Dr. Ann Cavoukian, the former Information and Privacy Commissioner of Ontario and an internationally recognized expert in the field of privacy, and Richard Alvarez, former President and CEO of Canada Health Infoway, in a piece entitled "*Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win".* While Dr. Cavoukian and Mr. Alvarez acknowledge that electronic medical records are essential to the provision of modern day medical care in a safe and efficient manner, they also articulate clear concerns about the privacy of such records:

> At the same time, the advantages of storing vast amounts of electronic information and the ease with which digitized information may be linked for authorized purposes present some of the greatest challenges to privacy and security, and to the continued widespread public acceptance of the EHR.[1]

The public relies on health service providers to maintain strict confidentiality of their personal health information. It is often extremely sensitive and very personal and can have real life consequences when it goes astray. While modern medical systems rely heavily on having immediate access to up-to-date information about their clients, in today's world the commodification of information and the ease with which it can be

---

[1] *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win* Dr. Ann Cavoukian and Richard C. Alvarez, March 2, 2012, p. 5

disseminated and shared, combined with the sensitivity of much personal health information, creates a situation in which the appropriate management of that information is vital. If the health system fails to ensure privacy and confidentiality it will erode trust and this erosion of trust will lead to individuals refusing or avoiding necessary health care. Achieving the right balance between having the right information available to the right health care provider at the right time and the right of the patient to maintain a level of control over their own personal health information is, therefore, essential.

Section 2 of the *Health Information Act*, which came into force in October 2015, provides that the purpose of the legislation is to address this balance:

> The purpose of this Act is to govern the collection, use, disclosure and protection of personal health information in a manner that recognizes both the right of individuals to access and protect their personal health information and the need of health information custodians to collect, use and disclose personal health information to support, manage and provide healthcare.

The Act applies to all records containing personal health information that are in the custody or under the control of a health information custodian as defined in the Act. The Northwest Territories Health and Social Services Authority has been designated as a health information custodian by Section 1 of the Regulations under the *Health Information Act.* As such, it must comply with the Act.

Section 8 of the *Health Information Act* requires health information custodians to establish or adopt and to follow "standards, policies and procedures" to implement the requirements of the Act and requires them to follow those standards, policies and procedures in the provision of health services to its clients.

The Act sets out the rules for:

- when a health information custodian can collect personal health information and the limits to what can be collected,
- how and in what circumstances that information can be used; and
- when and in what circumstances the information can be disclosed to a third party.

Section 10 requires a health information custodian to “take reasonable measures” to ensure that its agents (employees and contractors) comply with the Act. Section 11 requires that all agents of a health information custodian comply with the standards, policies and procedures established by a health information custodian and requires health information custodians to “take reasonable measures” to ensure that its agents comply with those standards, policies and procedures.

The viewing of personal health information in the EMR constitutes a “use” of the information, whether or not there is further use of the information by the employee or agent. Throughout the Act there are provisions which confirm that, while information can be used to provide medical services as needed, this does not authorize unfettered access to any health information by any employee of the health system. Rather, access to health information, including information in the EMR is to be used only on a “need to know” basis. This approach has been adopted by NTHSSA and is included in its training materials.

Simply saying it is so does not necessarily make it so. There are, however, a combination of tools in place to ensure that these directives are honoured and adhered to. They include administrative safeguards, technological safeguards and physical safeguards.

Administrative safeguards include such things as staff training, good policies and procedures and audits. Technological safeguards are things like firewalls, encryption, virus protection, and the requirement for user names and passwords. Physical safeguards include the use of privacy screens, the appropriate placement of equipment,

locked doors and file cabinets and alarm systems. None of these on their own will effectively protect information in the health sector, but used together they can effectively protect information.

In order to assist my own understanding of how the EMR works, I had NTHSSA provide me with a demonstration. This, in fact, is one of the reasons it has taken so long to produce this report because the NTHSSA had to create a module to demonstrate how the system works and to answer my specific questions without using actual patient information. My take-away from that demonstration was that the system is complex and nuanced and, at least to a point, flexible. The demonstration also provided me with a degree of comfort that the organization continues to adjust and revise and add roles and definition to roles as needed to meet the business needs of the health service providers.

1. Does the Roles Based Access, as set up, give too many employees access to too much information?

This question summarizes the first two of the Complainant's concerns. The focus of both is that too many employees have access to more information that what they need to do their work.

The Applicant alleges that all employees, regardless of the role assigned to them, have access to a basic "encounter record" for every client of the NTHSSA, regardless of where they live in the Northwest Territories. It is his position that even the most basic access to the system provides employees with access to sensitive personal health information including all of the reasons the client has accessed an appointment as well as information about any number of other medical facts about a patient including mental health diagnoses, participation in a methadone program, cancer treatments and abortions. He is also concerned that clinic assistants have access, in addition, to the Medical Summary Sheet, which includes access to a "problem list" and a list of medications used by the patient. He argues that too many employees have access to too much information and that NTHSSA has an obligation to do a better job of

restricting access to sensitive personal health information to only these who “need to know” to provide services to the patient.

As discussed above, access to the EMR is granted to each employee based on his/her need for that information to complete his/her job. Based on the demonstration of the EMR system provided to me, these roles appear to be fairly granular. Not all “clinic assistants” for instance are given the same access to the system. It will depend, in each case, on the specific job responsibilities of the specific employee. I am satisfied that NTHSSA is aware of the need to continue to adjust roles and the access that each employee is given in order to do his or her work. It is important that they continue to monitor and adjust these roles on an ongoing basis.

The health system in the north is not as compartmentalized as it is, for example, in a large urban centre. Particularly in our smaller communities where the receptionist might also be an interpreter and a file clerk, the job description for many employees goes beyond what might be expected of someone in a similar position in a large hospital in a large city. The job description for a “Clinic Assistant” for example includes reception, clinic support, records management and clerical support. They are, among other things, expected to:

- answer and direct telephone calls
- refer patients to the appropriate practitioner
- book practitioner referred specialist appointments
- collect and distribute documents coming and going from hospitals, specialists and labs
- perform pregnancy and urinalysis testing
- take and record electronic vital signs, recordings and other data such as height, weight and waist circumferences
- create and maintain client files
- administer requests for information from client files for review by practitioners (for example, to fill or refill prescriptions, and requests for information from external sources).

While clinic assistants may not need access to all of the information in the encounter record or the medical summary sheet for every patient contact, I am satisfied that the role of the position is such that they need access to more data points than might immediately appear obvious to someone not in that position.

Further, not every employee hired as a “clinic assistant” will be given the same access to information in the system. There are various levels of access given to various employees even with the same job title, depending on their specific responsibilities.

Finally, at some level employees and contractors must be trusted to comply with direction from the employer (the Authority) that they must restrict their access to only that information that they need to do their job for a particular patient or client at a particular point in time.

I am satisfied that the role based access system used by the NTHSSA is the industry standard for limiting access to personal health information and is an appropriate approach. It will not, by itself, prevent all unauthorized access to personal health information by system employees but it is an effective technical safeguard intended to help limit access. It works together with other safeguards, both technical (use of user names and passwords) and administrative safeguards (policies, procedures, training, auditing etc.). So long as the NTHSSA continually reviews and revises the roles and the access for all positions within the system and is actively managing roles so as to address privacy protection through the limitation of access based on the job description of each employee, they are meeting industry standards.

2. The use of random audits to help dissuade inappropriate access

The Complainant’s next concern is that while there are policies and directives in place which make it clear that employees “should” not look at any part of a patient’s health record unless there is a “need to know”, there are no enforcement mechanisms in place, such as random audits, to make sure that the policies and directives are followed. The Complainant does not feel that there are sufficient physical or

technological safeguards preventing employees from “snooping” and no routine auditing done so as to dissuade people from doing so. As a result, he says, patients are not aware of who, exactly, has access to their personal health information or how easy it is to gain such access.

The Complainant suggests that auditing of access to patient records is done in only two circumstances. The first is when the patient or client requests for an access audit on their records and the second is when a staff member accesses the name of a patient with the same last name.

The NTHSSA, however, assures me that there are many circumstances in which access audits are undertaken. For example, they may audit new users of the system to ensure they are using the system appropriately and not abusing their access privileges. I am satisfied that they have identified a number of criteria for conducting access audit and that these audits are not limited to the two circumstances outlined by the Complainant. Furthermore, all employees are warned, repeatedly, that these audits are conducted and that all of their activity in the system can be monitored. They note that the messaging around “snooping” is consistent and repeated through messages, and training. The “same name” audits are the ones where employees are often challenged to justify their access (because there are many people in the Northwest Territories with the same or similar last names) and it may be that this is the reason that employees know that “same name” audits are being done. But it is not the only instance in which audits are conducted. Just because employees are not aware of all of the circumstances in which audits are done does not mean they are not being done, or that they are not an effective way to control unauthorized access.

3. Employees viewing their own personal health information.

The Complainant feels that he should be able to look up his own personal health information but notes that if he does so it will be flagged and he will likely be punished for doing so. He feels that this is ironic when every other employee of NTHSSA system can see his EMR records at some level but he cannot.

While this may seem ironic to the Complainant, prohibiting employees from looking at their own personal health information is another “best practice” followed in most health care facilities. Under the *Health Information Act* custodians are restricted to collecting, using or disclosing only health information essential to carrying out the purpose for which it is being collected. Any use or disclosure of personal health information by any individual within a health service provider’s organization that is not essential to the provision of current care is, therefore, contrary to the Act. Employees viewing their own records is not essential to the provision of care. Employees do not, therefore, have access to their own personal health information. To allow access to employees would, among other things put third party personal information that might be in the records at risk or allow the employee to change his/her personal health records. Employees who wish to have access to their personal health records have the same rights to ask for those records as any other citizen.

The Applicant’s argument that virtually all other employees of the NTHSSA “could easily access this information with little chance of being detected/punished” is not an entirely accurate depiction of the system or how it works either. Access to all other employees is also restricted on the “need to know” principle. Just because fellow employees are able to look up a colleague’s information on the EMR doesn’t mean they will do so. The safeguards in place are intended to protect all patients, including employees who are patients, from unauthorized use and/or disclosure.

5. The “circle of care” as a model for permitting access to personal health records.

The Complainant argues that the concept of “circle of care” is still being used to justify the use of personal health information in the EMR by far more agents/employees of the NTHSSA than is appropriate or necessary. He is concerned that there are very different ideas about who should have access to a patient’s health information.

On this point, I completely agree with the Complainant. To the extent that the NTHSSA, or anyone employed with the NTHSSA, continues to use the concept of “circle of care” to justify the use and disclosure of personal health information, this must stop. There is

no reference in the *Health Information Act* to "circle of care" and the term does not accurately reflect the directions provided in the *Health Information Act* for the management of client files. It is clear, however, from some of the materials provided by NTHSSA with respect to this review that the terminology is being used. For example in a pamphlet entitled "*Protect Your Privacy within Electronic Health Information Systems"* published by the Government of the Northwest Territories Department of Health and Social Services a paragraph on the third page notes:

> Only staff and healthcare providers involved in your circle of care can enter, view and access your electronic medical information....

On page 4 of the same publication is the following:

> Your health information is private and only those staff in your circle of care can view and access the information they need to provide you with the best care.

Apart from these statements being misleading in terms of who is **able** to access an individual's personal health information, the reference to "circle of care" is used without any explanation as to what that term means. Any definition of "circle of care" will vary widely, depending largely on who is framing it. A patient will undoubtedly understand the term differently than a physician will. A physician may consider the "circle of care" to include every health care worker who may be involved in any aspect of the patient's care on a historical basis, while the patient might well understand his circle of care to include only the receptionist who signs him in, the nurse in the clinic who takes his blood pressure and the doctor who does the examination for a particular appointment.

The term "circle of care" has no place in policy, practice or mind set for health information management. The over-riding scheme of the *Health Information Act* is that, regardless of the ability of an employee to access a patient file, access to records is authorized only as needed for current care of the patient. As some have put it, "just because you can, doesn't mean you should".

I agree with the Complainant that the use of the term “circle of care” leaves the door open to and may even encourage inappropriate and unauthorized use and disclosure of personal health information. NTHSSA should, instead, be referencing “the right information to the right care provider at the right time”. No employee should have access any patient record or any part of a patient record unless the employee **needs** that information to provide medical services (or administrative support services directly related to the medical services) to the patient.

As noted below, much more work also needs to be done to educate patients with respect to how their personal health information is handled by health information custodians and about their rights in terms of their personal health information in order to ensure that patients have the ability to control, when necessary, access to their files.

6. Masking

The Complainant argues that the current EMR does not have the ability to "mask" - that is the ability to hide certain personal health information from specific EMR users.

Section 22 of the *Health Information Act* allows patients (with very limited exceptions) to place conditions on how their personal health information can be used or disclosed. When such a condition is placed, health information custodians must, among other things:

a) take reasonable steps to comply with the condition;
b) attach the condition to or record the condition on the applicable record or records; and
c) take reasonable steps to give notice of the condition to other persons and organizations to which information may be disclosed.

Similarly, section 24 provides that where a patient has provided express or implied consent to the collection, use or disclosure of personal health information, that patient

may withdraw the consent and the custodian must take appropriate steps as outlined above to respect the withdrawal.

The term “masking” has been used to describe a situation in which the EMR can be configured to prevent one or more employees from having access to any kind of information about a particular patient or to prevent all employees from seeing particular information within the client file. When the *Health Information Act* came into effect, the EMR did not have the technical ability to “mask” information without creating a myriad of other privacy issues. It is my understanding that this functionality is still not available.

During the course of this review, the NTHSSA did not address the Complainant’s concerns about masking. I have, however, raised the question with NTHSSA on a number of occasions over the last year or so. The last time I had the discussion, I was told that “masking” was not yet technically possible with the current EMR system. They conceded that, while they were working on a way to do this, masking was still not an option.

To me, one of the most important tools available to the public to manage who has access to their personal health information are the rights set out in sections 22 and 24. These sections provide a way in which individuals can place limits on who can see or use their records or give and withdraw consent to the collection, use and disclosure of personal health information. For example, if a patient does not want her nurse practitioner neighbour to have access to her files, she simply has to ask the custodian to put that condition in place. Or if a patient wants reference to a dated abortion hidden from anyone looking at the file, sections 22 and 24 allow a patient to give that direction to a custodian. There are some limits to what conditions can be made, but those limits are narrow. When a condition is place by a patient, the condition must be recorded on the patient’s file. Where appropriate, the Act also requires custodians to place a note on the patient file that pertinent information has been hidden, which alerts all health care providers that there may be additional information in the patient’s file that is relevant but for which they need the patient’s express consent to access.

The Act requires custodians to “take reasonable steps to comply” with a condition placed by a patient pursuant to section 22 or a withdrawal of consent under section 24. There is nothing in the Act which says what “reasonable steps” means or which requires a health information custodian to have “masking” functionality to comply with such a request. Without such functionality, however, the only way to comply with a patient’s specific condition in most cases would be to remove all of his/her records from the EMR system entirely. That, however, would also be contrary to the Act in that section 63 requires patient information to be recorded in the EMR system. This creates a clear dilemma for custodians and is something that needs to be addressed.

7. Psychiatric notes stored in the EMR

The Complainant is particularly concerned about who can view notes from the psychiatric nurses and psychiatrists with the out-patient program which are stored on the EMR. These notes contain detailed sensitive information and he claims that clients in the program are not aware that their notes are being stored in this “unprotected” way. He says that **all** service provider staff have access to such notes and that given the continued emphasis on collaboration and circle of care he is concerned that many service providers will see no issue in accessing these notes without client permission if they are working with the client in some other capacity.

I would first comment on the use of the word “unprotected” to describe the manner in which these records are being kept. All records in the EMR are protected to the extent that they are recorded in an electronic system with access controls and security protocols. I take the Complainant’s reference to mean that they are accessible by all employees or agents of the NTHSSA who have access to the EMR. It may be that within the system itself, these notes are viewable by more employees than really need to see them for the purpose of their responsibilities within the organization. That does not, however, equate to being unprotected.

The Complainant asserts that **all** staff, even those with the most basic access to the system, have access to these notes. If that is true, I agree that there is a problem that needs to be resolved. Unfortunately, NTHSSA did not directly address this concern in their response to me.

Much depends on the way in which notes are uploaded to the EMR. If there is only one way to upload information to the system and all notes, regardless of their origin, are uploaded to a page viewable by almost all employees, there is an obvious problem. If psychiatric notes are uploaded to a specialized module which is available only to physicians and/or nurse practitioners, depending on their role, the role based access model, combined with administrative safeguards (application user agreements, policies, procedures, employee training, professional standards, clinical standards, and codes of ethics) should, if applied, adequately address the concerns raised by the Complainant.

9. Forms used for referrals

The Complainant says that when physicians make a referral to the Community Mental Health and Adult Services (CMHAS) for a patient to receive counseling or out-patient psychiatry, they use the same form as they use if they were making a referral to a medical specialist - that is, they include a list of the patient's medical diagnoses past and present. He says this information is not required for client to receive counseling or psychiatric services and that having the information may undermine the counselor's or the psychiatrist's relationship with the patient.

Once again, this concern was not directly addressed by the NTHSSA in their response to this office. As I understand the system, however, a physician making a referral of any kind (including a referral to a psychiatrist or a counselor) will pull up the appropriate template on the system while in the patient's client file and that template will be automatically populated by things like name, address, contact information as well as previous diagnoses, visits, medical issues and medications. The physician would then provide it to the appropriate persons. I suspect that a physician pressed for time and

with the mind set that this is within the patient's "circle of care" might not bother to remove irrelevant information about the patient before finalizing the form. This is a process issue with a significant risk to privacy that must be addressed. As noted above, the primary and foremost privacy principle upon which the *Health Information Act* is based is that a custodian is to collect, use and disclose **only** the information required for the purpose it is collected, used or disclosed - the right information at the right time. If a counselor or a psychiatrist does not **need** to know information, it should not be provided in the referral form. If the counselor or psychiatrist decides that he/she needs more information, that information can be requested with the consent of the patient or otherwise in accordance with the Act.

10. Definition for the term "implied consent".

The Complainant says that, as an employee of the NTHSSA, he has not been given a clear understanding of what the term "implied consent" means.

The *Health Information Act* contains a plethora of provisions around the concept of consent for the collection, use and disclosure of personal health information. These provisions are convoluted and complex and difficult to understand. This is why a considerable amount of time is spent in the privacy training materials discussing the issue. In March 2017, the Department of Health and Social Services issued a directive requiring that all staff of all custodians receive mandatory privacy training within three months of the employee's start date for new employees with additional annual training for all employees, contractors, volunteers and information managers. The training materials do address the issue of implied consent and when a custodian can rely on implied consent. The *Health Information Act Guide*, which can be found at http://www.hss.gov.nt.ca/health/slides/health-privacy-protecting-your-health-information, has an entire chapter devoted to the issue of "consent". There are also a number of other resources available within the NTHSSA if the terminology is unclear and an employee needs clarification. Every employee should, therefore, have a basic understanding of the term "implied consent" and when it can be relied on as a result of

mandatory privacy training. There should, however, also be clear direction for employees in terms of who they can speak to in the Authority to clarify how the Act applies when questions arise.

11. The use of unencrypted email for transfer of personal health information

The Complainant alleges that personal health information, including counseling and psychiatric patient information is “commonly” sent and received through unencrypted email. He notes, as well, that it is not unusual for him to receive misdirected emails with a client’s personal health information but, when he reports such errors he is told that this does not constitute a breach because it was sent and received within the NTHSSA organization.

I have often addressed the use of fax technology and unencrypted email for communications which contain sensitive personal information, including personal health information and I have made a number of recommendations in the past aimed at addressing this issue.

The EMR has a secure internal messaging system and obviously this should be used, whenever possible, and following the established policies and procedures for electronic messaging, to communicate among employees of NTHSSA. When communicating with an outside agency, NTHSSA should be using the most secure method of communication available to them. I agree with the Complainant that, to the extent that personal health information is being sent either by way of unencrypted email or by fax, these practices have to change. They are not privacy protective.

In terms of whether or not an email or fax containing personal health information which has been misdirected within the confines of the NTHSSA organization is a breach of privacy, again I agree with the Complainant. Unless the recipient of such a communication has a “need to know” the information in the communication for the purpose of current treatment or care of the patient, a misdirected email with patient

information intact and readable constitutes a breach of privacy, even if it never leaves the NTHSSA organization.

12. Sharing of client information without clear consent

The Complainant alleges that there has been a practice among some counseling staff of sharing client information with other health care practitioners without clear consent. The context of these discussions, however, was not provided. The *Health Information Act* does allow for the use of personal health information without explicit consent in a number of circumstances.

Sections 34 and 35 of the *Health Information Act* set out situations in which a custodian can use personal health information. But even where a use is permitted, that use is still subject to adherence to the other requirements of the Act.

The list of permissible uses is extensive. For many of the listed uses, however, there is no **need** to use personally identifiable information about an individual to meet the organizational business requirements listed. For instance, while the facts of a particular situation might be properly used for the purposes of educating health service providers, it would be an exceedingly rare case where the patient in the situation needs to be identified to meet the educational goal.

As noted above, the over-riding principle is always “need to know”. Just because a custodian can use personally identifying personal health information for any of the permitted purposes, doesn’t mean they should. Over-riding section 35 is the obligation of custodians to use personally identifying personal health information only where there is a **need** for such an identification.

The “common practice” of sharing client information with other health care providers without clear consent is an acceptable practice under the Act only if those other health care providers have a **need to know** the details in a personally identifiable form for the

purpose of meeting the current medical needs of the patient. The issue here lies not in whether or not practitioners and employees can discuss client files and client situations, but in whether or not those discussions identify the patient and in whether all of the parties to the discussion **need to know** the identity of the individual involved.

It should be noted, as well, that what the Act allows and what a professional governing body might think is acceptable ethical practice may not always mesh. There are some medical professions (including counseling and psychiatry) in which the need for explicit consent of the patient to the disclosure of personal health information is more strongly entrenched than in others. Where those standards are higher than those required by the *Health Information Act*, and are not in conflict with the law, those are the standards that should, where possible, be adhered to.

13. Lack of patient education

Many of the concerns raised by the Complainant in this matter pointed to the lack of "patient education" about patient privacy rights and about how personal health information is handled in a modern electronic record keeping system. Most patients simply do not know how health information flows within the system or what kind of information is being stored in their EMR. Most do not know that they can request a copy of their EMR records or that they have a right to know who has looked at their records. They generally do not know what kind of information is "appropriate" for a health care provider to be collecting and placing on a permanent health record or what, if any, limits there are to what can be placed on the EMR. They do not realize how many health professionals are able to access their records (whether or not they do) or in what circumstances any particular health care employee might need to see their records. They do not know, except in the most rudimentary way, what the *Health Information Act* allows in terms of the collection, use and disclosure of their personal health information. They do not know that, in order to limit access to their personal health records in any way, the onus is on them, the patient, to make the request.

I agree with the Complainant that much more needs to be done to educate the public about their rights under the *Health Information Act*. While some materials have been prepared, those materials are either out of date, misleading or so basic that they do not relay the entire set of rights a patient has. Many of the materials are hard to find on-line. There are posters with minimal information posted on the walls of at least some primary health care offices but there is little on those posters that educate the public about how they can exercise their rights. There was only a rudimentary advertising campaign in the lead up to implementation of the *Health Information Act* and, to my knowledge, no ongoing publicity to provide the public with a clear and thorough understanding of how the *Health Information Act* affects them.

CONCLUSIONS AND RECOMMENDATIONS

I am impressed and encouraged that the Complainant in this case has taken it upon himself to question the privacy policies, practices and procedures within the NTHSSA. While not all of his concerns are necessarily well founded in terms of the legislation, his ability to identify and flag potential privacy issues is encouraging. I would encourage HRHSSA to collaborate with its employees, particularly those who express an interest in the subject of privacy within the organization, to work toward the most privacy protective environment possible.

Based on the above discussion, I make the following recommendations.

1. I recommend that NTHSSA continue to monitor and adjust access to the EMR as necessary based on the job description of each employee;

2. I recommend that NTHSSA continue to do regular access audits and to monitor situations in which “snooping” are more likely to occur. Further, I recommend that NTHSSA continue to send consistent and frequent messages to all of its employees (including physicians) aimed at dissuading them from viewing or otherwise using any information about any patient/client unless absolutely necessary to complete their jobs.

3. I recommend that NTHSSA continue to prohibit employees from viewing or accessing their own records in the EMR and to monitor employees to prevent same.

4. I recommend that NTHSSA review all of its public education materials and remove all references to the term “circle of care” and amend them so that these materials more correctly explain the system on the basis of “need to know” and “the right information about the right person at the right place and at the right time”.

5. I recommend that, to the extent that NTHSSA still uses the term “circle of care”, this concept be immediately and permanently removed from all parts of the NTHSSA organization. I further recommend that NTHSSA re-educate its staff using the more appropriate “need to know” terminology and focus, emphasizing that access to a client file without a current “need to know” will constitute unauthorized access and will invite disciplinary action. This recommendation would apply equally to all health information custodians, including the Department of Health and Social Services.

6. I recommend that NTHSSA take immediate steps to give honest and true effect to sections 22 and 24 of the *Health Information Act*, whether by way of an electronic solution (masking) or some other consistent and effective process. The current policy directive from the Department of Health and Social Services (Consent Conditions Policy) does not provide appropriate direction on how to achieve this. These provisions are absolutely foundational to achieve the purposes of the Act. At the very least, NTHSSA has to develop practical procedures and practices that will allow it to comply not only with sections 22 and 24, but also with section 65 which requires a health information custodian to use the EMR for medical record keeping. Health information custodians cannot place more importance on one section of the Act (the requirement to document in the EMR) than on another (the patient’s right to control the collection, use and disclosure of personal health information). Both sections must be complied with

and if the system itself does not have the appropriate functionality, another way must be created to comply with both sections.

7. I recommend that NTHSSA examine how notes from psychologists and psychological nurses and counsellors (to the extent that counseling notes are uploaded to the EMR), are uploaded to the EMR and ensure that they are compartmentalized in a fashion that restricts access to only those who have a legitimate need to see that information. This kind of information is not the kind of information which should show on up on the front page of the EMR system any time any employee logs in to a patient's file. If there is a need to allow access to one or two front line staff to receive and appropriately file such notes, those specific staff should be given the necessary access to such notes, but it is inappropriate for all staff to have "unavoidable access" to such information on a patient file.

8. I recommend that NTHSSA provide direction to physicians and others who make referrals to specialist or other health services with respect to the appropriate amount of information to be included in the referral documentation. If there is no clear need for the specialist to have information about previous diagnoses or about current medications, that information should not be included in the referral forms. Physicians should, at the very least, be putting their minds to how much information is actually necessary to impart to the specialist in the first instance for each client and be limiting the disclosure to the least amount of information that is necessary for the specialist to understand the client's needs. If the specialist or other care provider finds that more information is required, that can be dealt with subsequently with the consent of the client.

9. I recommend that NTHSSA provide all of its employees with clear messaging that invites questions about any privacy matter from employees/agents and provides all employees/agents with the name and contact information for those within the Authority who are subject area experts and who are knowledgeable

about these matters so that when an employee is unclear about a privacy issue, they have a resource from which they can draw.

10. I recommend that NTHSSA develop and enforce policies which direct all of its employees/agents to use the most privacy protective tools available to them when communicating information about patients. This policy should include a hierarchy of appropriate means of communication, with the use of internal systems at the top of the hierarchy and a requirement to encrypt or password protect communications whenever possible.

11. I recommend that NTHSSA make it clear to all of its employees and agents that a misdirected communication containing personal information or personal health information is a breach of privacy, even if the misdirected communication originated and ended within the Authority.

12. I recommend that NTHSSA add reminders in their regular and ongoing messaging to employees and agents about their obligations under the *Health Information Act* to maintain the confidentiality of patients and clients and that discussions between employees be kept on a "need to know" basis and, for the purposes of mentoring or consulting another practitioner, the identity of the patient/client should, where possible, remain undisclosed.

13. I recommend that the NTHSSA and/or the Department of Health and Social Services create and disseminate a public education campaign to educate the public about how the *Health Information Act* affects the patient, and outlines the patient's rights under the *Health Information Act*, including, most importantly, the right to place conditions on how their personal health information can be collected, used and disclosed and the right to withdraw consent to the collection, use and disclosure of personal health information. This public education

campaign should be presented over time and on a variety of platforms, including social media.

Elaine Keenan Bentgs
Information and Privacy Commissioner