NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 12-104
11-155-4
March 26, 2012

THE COMPLAINT

In June, 2011, I received a complaint from an individual who works within the organization known as Yellowknife Health and Social Services Authority (YHSSA). This person (who will be referred to in these recommendations as A.B. for ease of reference) was extremely concerned about what he considered to be "inadequate protection of my medical information" by YHSSA.

A.B. indicated that an Electronic Medical Record (EMR) known as "WOLF" was put into place with the opening of the new Yellowknife Primary Care Centres in June 2010. He says that numerous staff from different disciplines (clinical assistants, administrative staff, nurse practitioners, licensed practical nurses, mental health counselors, physicians, supervisors, management, information technicians etc.) use this system. All of these people, he said, have easy access to information within the EMR and although some staff have more access than others, all staff can readily access sensitive information such as the reason for patient visits. Furthermore, he said, there are no safeguards in place to *prevent* inappropriate access to sensitive patient information and no "alarm" which would identify when information has been improperly accessed. According to A.B., there is no routine auditing done on the system. It is A.B.'s observation that the EMR was implemented first and only after that were privacy and security issues addressed, rather than ensuring that privacy was built into the system from the beginning.

It is A.B.'s assessment that the implementation of the EMR without having first addressed these privacy issues have dramatically increased the risk of inappropriate use and/or disclosure of very sensitive health information because the number of

people who have easy and apparently unmonitored access are greater and the ease of access is increased because accessing a computer file can be done more discretely than pulling a physical file.

BACKGROUND

In Canada, visions of an interoperable electronic health system which would allow medical personnel to access an individual's medical health information from anywhere in the country have fueled the explosion of new systems for the electronic storage of medical health information. Quite literally billions of dollars have been spent on the creation of electronic medical systems from coast to coast. As almost anyone in the medical profession will tell you, EMRs are the future of health care in Canada. 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.

In a more recent publication entitled *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win*, co-authored by Richard Alvarez, President and CEO of Canada Health Infoway and Dr. Ann Cavoukian, Information and Privacy Commissioner for Ontario and an internationally recognized expert in privacy issues, the authors make the following observation:

> 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]

Every jurisdiction in Canada is dealing with these issues. Most Canadian jurisdictions have recognized that medical health information and the collection, use and disclosure of such information, raises many issues that do not generally arise with less sensitive or less complex systems. These jurisdictions realize that there are a large number of variables that simply cannot be addressed through basic access and privacy legislation, such as the *Access to Information and Protection of Privacy Act* (ATIPPA). While most Canadian jurisdictions have passed health specific privacy legislation to address the nuances that surround health information privacy, the Northwest Territories has not yet done so. The governing legislation for now, therefore, is the ATIPPA. I will refer to the specific relevant sections of that Act later.

THE "WOLF" SYSTEM

Upon receiving this complaint, I wrote to YHSSA and asked them to provide me with a detailed description of the WOLF system, how it worked and what privacy protections had been implemented in the system. Specifically, I asked them to answer the following questions and provide the following information:

a) a detailed description of who has access to personal information within the system and how that access is controlled;

b) assuming that role based access is the basis of the system, a detailed description of how the roles are defined and the specific information which each role has authorization to access;

c) how are the "roles" determined and who, if anybody, is responsible for reviewing those roles and assigning them to individual employees;

---

[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

d) what criteria is applied to determine which role is assigned to each employee;

e) is there a clear provision for revocation of authorization for users who cease working for the clinic or who improperly access records in the system;

f) do health care workers outside of the clinic have access to clinic records? If so, in what circumstances;

g) is there an "override" function within the program which would allow someone not otherwise authorized to access information beyond their "role"

h) if so, how does that override function work and is there any automatic flagging of the transaction such that it will be caught contemporaneously with or almost contemporaneously with the event;

i) what audit functions are built into the system and how are those audit functions used, including who is responsible for audits, how often routine auditing is done, and how an anomaly would be flagged and/or dealt with once flagged;

j) what happens if a user "forgets" to log out on a particular computer;

k) how are passwords controlled - for example, is it possible for a doctor who has access to all or most of the EMR to simply give his/her password to a receptionist or nurse, thereby giving them access to records they wouldn't otherwise be entitled to?

l) has a Privacy Impact Assessment been done with respect to the EMR

m) what is the consent model which the EMR is built on (express consent, implied consent, no consent?)

n) what training has been done for personnel working on the new system

o) what information is/has been provided to the public with respect to the new EMR and how it works

In their initial response to me, YHSSA provided me with the following information about the system:

- The EMR system operated by YHSSA is currently used in both Yellowknife clinic sites. It does not appear to be “interoperable” between the two sites such that someone in Clinic A can access the records of a patient who has seen a doctor in Clinic B, but it appears that staff (other than practitioners) rotate between the two clinics so that the number of people who have access to information in the system is about 143 people.

- those who have access to the system include 5 mental health/addictions counsellors, 8 administrative assistants, 18 clinic assistants, 8 billing clerks, 12 LPN’s, 24 RN’s, 6 managers, 4 records clerks, 1 quality risk management co-ordinator, 2 diabetes educators, 1 dietician, 1 medical social worker, 54 medical practitioners and 4 IT department employees.

- each of these employees has received training in the use of the system, including a briefing about confidentiality and what constitutes appropriate access

- access to the system is controlled by the use of individual and unique user names and passwords. Employees are “advised not to share their passwords with anyone”.

- all employees sign a confidentiality agreement when hired

- to log on to the EMR the user must first log on to the YHSSA network, which is also username/password protected.

- individual sessions are “timed out” after a set period of inactivity (there was no indication how long that period was) and the user is then automatically logged off the system

- access to the system is controlled by a “role based access” paradigm. “Roles” are defined by an employee’s job description so that, for example, a physician

may have access to the entire record, but the receptionist can only see more limited information about the patient (name, address, medical complaint, medication). The YHSSA IT team assigns access to the system based on the job description.

- it is not possible to access the system outside of the GNWT network without a VPN network connection

- it is possible to “lock down” a patient’s information such that it is available only to the employee who created the record, though this function is not widely used as it is considered to be counter to the core purposes of the EMR, which is the effective sharing of information to support the provision of comprehensive collaborative health care

- when an employee leaves the employ of YHSSA, revocation of access to the EMR system is part of the standard closure procedure.

- at the time of it’s response (July, 2011) YHSSA indicated that they were “in the process” of implementing a routine EMR auditing process

- the EMR itself is designed with “robust” audit functionality that records the action and identity of the user every time the system is accessed. This enables the review of concerning cases should they arise and allows for the establishment of a routine auditing protocol

- when the routine auditing process is in place, it is anticipated that it will be the Quality Risk Management Co-ordinator who will conduct the audits. A policy clearly outlining the audits to be performed, the details with respect to conducting, monitoring and reporting as well as the proposed actions in the event of proven inappropriate access was under development

- a public information pamphlet with respect to the move to an EMR system was developed and made available to the public but there does not appear to have been any more aggressive attempts to educate the public about EMR's or the benefits and/or risks associated with such a system. YHSSA does not seek individual express consent from patients before moving them to the new system.

- in order to improve access to practitioner services, YHSSA has implemented a new delivery model wherein clients are not "tied" to one practitioner. The ability to provide a client appointment with an available practitioner within the clinic when their primary care provider is unavailable is made possible through the availability of information contained in the EMR and the fact that that information is accessible by other practitioners

- unless precluded by legislation to the contrary, as in the case of child protection legislation, YHSSA takes the position that they, as a Health Authority, can share client information within the Authority as needed to facilitate their functions, without client consent.

When provided with the public body's first response as noted above, the Complainant had some concerns about the way in which YHSSA explained the system. He wanted, in particular, to elaborate on the significance of the "Encounter Record" which is found on the Medical summary page of the EMR for all patients and which is accessible to all users of the system, regardless of the "role" they are assigned. This record is available when the medical summary is entered, when any client is booked for any reason and when any staff person makes a note about the visit. A.B. says that the information on this page can be quite sensitive - for example, the following things could well appear on this page:

- pregnancy
- substance abuse
- erectile dysfunction
- cancer screening

- therapeutic abortion
- psychiatric diagnosis - Bipolar Mood Disorder, Schizophrenia, Panic Attacks
- Sexually transmitted disease screening

This information is, therefore, unavoidably available to all staff, up to 143 people.

A.B. also has concerns about the "role based" access protocol, most particularly the access available to clinical assistants. Between the time that A.B. filed his request for review with my office, and the date of his response to the comments provided by YHSSA in August, it appears that some changes had been made to the systems. Prior to that, staff had been told that the WOLF system did not allow for removing Clinical Assistants from having access to the Encounter Record. At the time of the response, however, changes had in fact been made so that "most" clinical assistants no longer had such access, though it appears that this has not been fully resolved. He was further concerned that for mental health/addictions counselors, all appointments are required to be "booked" through the EMR system. Each time this is done, the counselor will see the Encounter Record and cannot avoid seeing the list of reasons for the client's previous medical encounters. So, for instance, it may be that an individual is seeing a substance abuse counselor and the counselor sees from the EMR that she is also pregnant, but the client doesn't offer that information to the counselor voluntarily. This kind of information would put the counselor in a very difficult position both professionally and ethically.

On the flip side, although regular scheduled counseling notes are not inputted into the system other than a notation to "see paper file", every day there are two to three "same day" counseling appointments offered. These are "drop in" and often one time only sessions. For these sessions, the counseling staff is directed to put the full notes from these sessions into the WOLF EMR. Although not available to all staff, this makes the counseling notes available to a large number of staff.

A.B. also points out that with integrated services, any physician can now provide services to any client. As well, the client may access other services. For different reasons, a client may not want all physicians, nurse practitioners, LPN's, dieticians and administrative staff to know that he/she is, for instance, obtaining counseling. With the WOLF system, however, the client won't have control over who sees the record and will not likely even be aware that the entire staff, potentially, has access to this information.

Finally, on this issue, A.B. points out that although YHSSA has apparently figured out how to block the medication list that is found on the medical summary sheet beside the Encounter list so that that information was not generally available to all staff, the block has not been generally applied but has been blocked from only to a few of the counselors. IT staff did not implement the block for all counselors because "no one asked them to". Essentially they were told that if they wanted the block they had to ask for it rather than management taking responsibility for making this an automatic block for employees who had no need to access certain information.

With respect to training, A.B. commented that in his estimation, the briefing provided to staff about keeping information confidential is minimal, at best.

Concerning the issue of patient consent, A.B. commented that if he had not been an employee of YHSSA, he would not have known how many people have access to his health information within the clinic. Of particular concern to this individual was that clients who receive counseling services are not aware that the Director of Social Programs has access to counseling notes, and that the Director is also responsible for the Child and Family Services program (child protection services).

THE REPORT

In November, YHSSA provided me with a letter which indicated that, after receiving my initial correspondence with respect to this complaint, and after taking the time to

articulate their original response, they decided that they would request a legal review of the EMR from their counsel. As part of that legal review, legal counsel conducted a Privacy Impact Assessment and made a number of recommendations which they have committed to addressing in their current and future planning. A copy of the report entitled "Review of Issues Surrounding Electronic Medical Records & Privacy: Creating an Action Plan for Moving Forward" (the "Report") prepared by legal counsel was provided to me. Although I appreciate the effort that was put into the Report, I am concerned that the conclusions reached do not accurately reflect the current state of the law or address the concerns that patients will have about the privacy of their personal medical information. For that reason, I will refer extensively to the Report and provide my comments.

The Law

The Report quite correctly points out that Canadian courts have long recognized privacy rights in regard to one's personal information and that "informational privacy" has been defined as "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself"[2]. This is an important definition that should be kept in mind, front and foremost, in all of the discussions with respect to the EMR. The Report also refers to the Supreme Court of Canada's recognition of the special sensitivity of health information in the case of *McInerney v. MacDonald* [3] where the court stated:

> Medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient.

---

[2] *R. v. Duarte* [1990] 1 S.C.R. 30 at 46

[3] [1992] 2 S.C.R. 138 at 149

And further:

> ....certain duties do arise from the special relationship of trust and confidence between doctor and patient. Among these are the duty of the doctor to act with utmost good faith and loyalty, and to hold information received from or about a patient in confidence.

I full agree with these statements. However, this is where the author of the Report and I begin to diverge in terms of our opinions of the law. The Report states:

> Consent to access to such information is usually expressed. However, it can also be implied. Patients understand that their personal health information will be shared within the "circle of care". Industry Canada states that the "circle of care"
>
> > ...includes the individuals and activities related to the care and treatment of a patient. Thus it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultation with other health care providers
>
> This circle of care would include all those who carry on activities related to the provision of health care. It would include the clerk who arranges for an appointment; a medical assistant who checks a client into an examination room and takes vital signs; a nurse who helps a physician with a procedure; and, everyone else who assists with client care. It does not allow for unlimited access to client information. Rather, access is given as necessary to perform job related activities and duties.

There are a number of problems with these statements.

Firstly, and most importantly, our legislation does not refer to a "circle of care". This is a concept which has been used in health specific privacy legislation in some Canadian

jurisdictions. In each of those jurisdictions the specific definition given to the concept is different and the concept is used to define the group within which personal health information can be shared for the purpose of providing medical assistance. Even with a definition for the term, those jurisdictions are finding that the general public and health care providers are interpreting the scope of the concept very differently. Here in the Northwest Territories, we do not have the benefit of even a flawed definition of the term. In the opinion of Gary Dickson, the Information and Privacy Commissioner of Saskatchewan, even where there is a legislated definition of "circle of care", the terminology is, in fact, not very helpful. In his opinion, it may be used to help explain to a patient or layperson the flow of personal health information in very basic terms but he feels that it is unhelpful when it comes to training of health care workers who should have a far more nuanced understanding of when and how sharing of personal health information can occur. [4]

Secondly, the *Access to Information and Protection of Privacy Act* provides that personal information can be "used" or "disclosed" in only narrowly defined circumstances. In the context of personal health information, information collected can only be used for the purpose for which the information was collected or compiled, or "for a use consistent with that purpose"[5]

In my opinion, if the term "circle of care" is to be used at all, it must be used with this section of the Act as the basis of any discussion of what constitutes the "circle of care". Keeping in mind that one of stated purposes of the *Access to Information and Protection of Privacy Act* is to prevent the unauthorized collection, use or disclosure of personal information by public bodies (Section 1 (d)) it is my opinion that the question of what might be a "consistent purpose" must be measured from the point of view of the

---

[4] *Glossary of Common Terms - The Health Information Protection Act,* www.oipc,sk.ca

[5] Access to Information and Protection of Privacy Act, S.N.W.T. 1994, s. 43(a)

patient, not the public body. So, for instance, if I attend the doctor's office on Monday to deal with a broken bone, I would not anticipate that the record that is created of that event would necessarily be available to my dietitian when I go in next week to deal with a dietary issue, or to my counselor when I attend mental health counseling. I most certainly would not anticipate that my personal health information would be available to the Director of Social Programs for any purpose. For most people, their understanding of a "circle of care" is far narrower than the current EMR allows for within it's current configuration, particularly in light of the very wide range of services provided in each of the two clinics which run WOLF. From the patient's perspective, dealing with a broken leg and dealing with a dietary or mental health issue would not necessarily be consistent purposes. The reasonable person would likely concede that there is an expectation that there will be a certain number of individuals who will be involved in treating a broken leg:

- the nurse in attendance
- the X-ray technician
- the doctor who sets the leg

and each of these individuals will require access to some information about the patient so that the broken leg can be dealt with. In my opinion, this is how the patient would define the "circle of care" for dealing with a broken leg. Within this "circle of care" an implied consent to the sharing of related personal health information can be reasonably inferred, as the information is all being used for a purpose consistent with the reason it was collected - to diagnose and treat the broken leg. To assume, however, that that implied consent extends so as to allow a different practitioner to review the information for the purpose of dealing with a totally unrelated matter goes well beyond the scope of "consistent purpose" as used in our current legislation.

So, to the extent that the Report prepared for YHSS suggests that once personal health information is collected, the "circle of care" extends to all and any health issue that

might arise, I strongly disagree. Unless and until the patient fully understands the ways in which his/her personal health information will be used beyond the presenting complaint, and has been given the option to request that certain information be restricted, the implied consent should be narrowly interpreted to focus only on the complaint which sparked the visit in the first place.

The Report indicates that since the filing of the complaint which sparked this review, steps have been taken to block access to the counseling records. This specific complaint was focused on the degree of access to counseling records and the degree of access that counselors had to other personal health information of the patient. Now, the appointments are logged in, but except for those booking appointments and the counselors, the WOLF Workdesk will show only a note in regard to the appointments which says “Unavailable Due to Security Restrictions”. The Complainant did recognize that there had been changes to the system since he first submitted his complaint to my office which had the effect of hiding most counseling notes from general view. However he had originally complained that there are some instances in which the notes are required to be posted in WOLF and it is unclear from the Report whether this is still the case. Furthermore, it is unclear from the Report how many people have access to the system to enter appointments and therefore have access to the more detailed record. Nor has the public body addressed the issue of counselors having unavoidable view of other medical information which appears on the Encounter Record of the patient, which may have the effect of compromising the counselor/patient relationship.

The ATIPP Complaint

At page 6 of the Report, the following statements are made:

> In regard to medical records, they are accessed by staff as they fulfill their respective functions as part of the “circle of care”. There is implied consent to access the client files, but access is only as necessary to

> perform duties, and staff always have a duty to maintain confidentiality as they perform their functions.

It goes on to state that:

> Everyone in the circle of care plays an important role. As part of that, some of the information they request may seem, on the surface, to be intrusive and unnecessary. However, when one understands the full context, it makes perfect sense.

Part of the problem is that patients rarely "understand the full context" in which their personal health information is being used or viewed. There are undoubtedly a lot of good reasons for a receptionist to collect certain information when an appointment is being made. The issue is not the collection of the personal information - the issue is how that information is used and disclosed after it is collected. If it is collected by the receptionist to ensure that the patient is paired with the appropriate doctor for his/her needs, that is a use that a patient would expect it to be used for and the consent is, therefore, implied for that purpose. The question is how far beyond that can the information be used and/or disclosed before the consent can no longer be implied. The Report quotes from a paper prepared by the University of Alberta, Health Law Institute and the University of Victoria, School of Health Information Science prepared in 2005:

> "...to require express consent for every use and disclosure of a patient's information via EHR within a circle of care would likely grind health care delivery to a halt and undermine the very benefits that EHR's were designed to provide"[6]

The Report goes further and suggests that "it is unlikely that a health care provider has

---

[6] *Electronic Health Records and the Personal Information Protection and Electronic Documents Act*, April, 2005

the time or technical knowledge to have a lengthy conversation with clients about the EMR system". If a health care provider does not have the technical knowledge to explain the use of the information in an EMR, it is certain that a layperson will not have the requisite understanding from which a widely based, overarching implied consent to the use of personal health information can be assumed. While I agree that there is a certain parameter within which an implied consent to the use of personal health information can be assumed because it relates to the purpose for which the information was collected, that implied consent has a fairly narrow application under the *Access to Information and Protection of Privacy Act*.

One of items listed in the Report's "Action Plan" was to have YHSSA officials "continue to work on ways of ensuring client privacy and confidentiality in the EMR system" and to "develop educational materials to educate the public on the EMR system and its role in providing quality health care". While these are appropriate actions, I suggest that before that can be done, there is far more work to be done to define the appropriate uses of personal health information and the limits of "implied consent" within the context of the large, multi-discipline clinics in the YHSS system. If the term "circle of care" is to be used, it must be defined, not in the context of what works within the EMR, but within the context of how a reasonable person using the system would define it.

Where Implied Consent Does Not Exist

The Report goes on to talk about situations in which there is no implied consent. This section, too, causes concerns from the perspective of the patient. According to the report:

> Yellowknife is a small community. As such, it is realistic to expect that there will be occasions when a client does not give implied consent to health care workers at the Yellowknife Primary Health Care Centre to access to his or her file for the purpose of providing care. There have, in fact, been occasions where a client has expressly requested that a certain person or persons not be able to access his or her file.

> It is possible to lock down the system such that only one person, such as the treating physician, can access the patient's file. However, while this is possible, it has the potential of impacting the care of the client in a huge way. For example, if you could not see that particular physician, no other physician would be able to assist you, even for simple appointments for things like medication refills. Also, another physician would not be able to review chart information to consider past test results, diagnosis, medications, etc.

Once again, this approach does not adequately address the issue from the point of view of the patient. Clearly, if the only way to "protect" a patient file from unwanted access is to limit access to only one person, the system itself (WOLF) is insufficient to the meet the requirements of YHSSA. If this technology is such that you can restrict access to a file to only one person, surely the technology is available to prevent one person (or two, or three or four particular people) from having access to a file. If WOLF is unable to do this, then a new system should be considered. I suspect, however, that with a little ingenuity and some tweaks, the technology can be "trained" to do pretty much whatever YHSSA asks it to do. There is, however, no world in which the technology should be dictating the needs of the system. The technology must be sufficient to address the needs of the system, not the other way around.

I am troubled, as well, by the implication contained in this part of the Report that suggests that all personal health information in the system can be used for any "health related" issue under an implied consent UNLESS there is an express request made by the patient to limit that consent. If anything, it seems to me from the patient perspective, and in the absence of any health specific privacy legislation, the default really is a requirement for express consent unless the patient approves a more general implied consent. This is particularly so where it appears fairly clear from the discussion that the public has really received no information about the system and how it is used. If you don't know you have to ask, you won't ask. If you don't understand how widely your personal health information is being used, you are not in a position to consider

whether or not you feel comfortable with that situation. You no longer have the right, as an individual, to determine for yourself when, how and to what extent you will release personal information about yourself.

YHSSA has identified the need to continue to consider ways of locking the system down to protect a client's confidentiality while at the same time affecting the ability to provide client care to the least extent possible. My concern, however, is that the right of patients to control the use of their own personal information is clearly being given a back seat to the convenience of the system. From the patient's perspective, the priority must be to give the patient the ability to control who has access to his/her personal health information. The technology should be there to support better health care to the patient. It shouldn't, however, be the technology limiting the individual's right to decide how his/her personal health information is being used.

The Philosophy of a Primary Health Care Centre

At page 9 of the Report, the following statement is made:

> One of the guiding principles behind the creation of a primary health care centre is that a group of care providers, working together, can provide the best possible care to clients. This continuity of care philosophy includes the sharing of information to best meet the needs of clients.
>
> In an ideal world, this would mean that all care providers, including physicians, counsellors and mental health workers, would have access to the full client file.

And later

> It is the view of YHSSA officials, that if clients knew the benefits of such disclosure of information, they would likely consent.

The Report acknowledges that “a patient’s interpretation of ‘circle of care’ may differ from that of health care provider’s”. They conclude that

> ...it makes sense for YHSSA officials to consider options for obtaining consent for fuller sharing of information. This might include the following:
>
> - perhaps there should be educational materials that explain the EMR system and the benefits of information sharing
> - development of a consent for release of information that includes a number of options available to clients in terms of the extent of the consent (ie. a patient may consent to the physician knowing whether or not the client attended appointments with the mental health counsellor but may not want any notes from those appointments to be disclosed);
> - any possible options regarding the extent of the consent would have to be considered in the context of the EMR - what is, and what is not, possible from a technological perspective

It seems to me that the effectiveness of any system depends on how much trust the patient has in it. In the words of Gary Dickson, the Information and Privacy Commissioner of Saskatchewan:

> Given the prejudicial nature of personal health information, there may be no arena where privacy is more important than that involving diagnosis, treatment and care of patients. There are already a percentage of patients who refuse to disclose certain health history to their primary care providers. As Saskatchewan constructs an ambitious and expensive EHR system, it will be important for trustees to demonstrate that patients can be confident that their privacy will not be at risk with the move to electronic

> records which may be accessible by many more individuals than was ever the case with paper records.[7]

Rather than simply "considering options", I would suggest that YHSSA needs to find solutions which allow the patient the right to control the use of his/her own personal health information. Considering options is simply not in keeping with the legal requirements set out in the *Access to Information and Protection of Privacy Act*.

It is a recurring theme of this discussion that the technology appears to be dictating the parameters of how much control the individual will be able to retain over his/her personal health information. This is a relatively new system. The Government of the Northwest Territories and the Government of Canada are investing significant amounts of money into developing Electronic Health Records, not only for those who use the Yellowknife clinics, but for all those who use the NWT Health Care System. This is technology that will, in theory, manage our personal health information well into the future and set the parameters for a Territories wide (and, eventually, a country wide) interoperable health care system. It seems to me that we need to build it right the first time. Why would we let the technology dictate the parameters of how it can and cannot be used? As the system is built, it must recognize that this is the patient's information and that the patient is entitled to control how that information is used and who can see it. The system needs to be built, from the ground up, as a system that fits the needs of the medical profession AND respects patient's autonomy and right to make decisions for themselves. Right now it appears that the system being built is one that meets the needs of only one side of the equation.

<u>Maintaining Privacy and Confidentiality - Prevention of Unauthorized Access to Personal Information</u>

The Report outlines the measures currently in place to prevent the unauthorized access

---

[7] Investigation Report H-2010-001, Office of the Information and Privacy Commissioner, Postscript. March 23, 2010

to patient information from those inside or outside the YHSSA system. It points out that every employee is required to provide an Oath/Affirmation of Secrecy upon being employed by YHSSA. This oath/affirmation makes it clear that confidentiality is expected of all YHSSA employees and that failure to maintain that confidentiality could result in disciplinary action, up to and including dismissal. The Report quite rightly points out that:

> It is one thing to have employees complete and oath/affirmation. It is another to ensure that employees understand the complexities of privacy and confidentiality in the workplace. This is particularly true given the sensitive nature of medical and counseling information.

To address this, the Report states that all new employees at YHSSA have a discussion with their manager in regard to privacy and confidentiality issues. Further, the Report says that steps have been taken to ensure that staff have the opportunity to participate in sessions regarding privacy and confidentiality. There is no indication as to how often these opportunities are presented, nor whether there is any compulsory training in this regard.

The Report points out that YHSS is a public body and, as such, its employees are subject to the *Access to Information and Protection of Privacy Act*. They argue that the Act provides additional limits on employees in the collection, use and disclosure of personal health information. The Report points out that a failure to protect the privacy, confidentiality and security of personal information could result in the employee being named in a lawsuit for damages, or being implicated in a complaint under the ATIPP Act. The Report refers, as an example, to a situation which occurred in Calgary, Alberta, where a medical clerk improperly accessed another person's personal medical information and was fined $10,000.00 and a similar case in Ontario in 2010. Fortunately for both of those jurisdictions, the existence of health specific privacy legislation provides for specific remedies for custodians of personal health information who fail to live up to the obligations imposed on them by the legislation. Although we

have privacy legislation, it is generic in nature and the Information and Privacy Commissioner of the Northwest Territories has no power to impose sanctions or penalties or, for that matter, to do anything other than make recommendations. Section 59 of the Act does provide that it is an offence to knowingly collect, use or disclose personal information in contravention of the Act, but this requires that the individual be prosecuted and the penalty is limited, on conviction, to a fine not exceeding $5,000.00.

The Report also points out that health care professionals can be reported to their regulatory bodies and could face disciplinary actions. Not all employees who have access to the WOLF system, however, are members of professional regulatory bodies.

Finally, the Report points out that the EMR has a “robust functionality that records the actions and identity of every actor in the system” which “enables the review of concerning cases should they arise, and allows for the establishment of a routine auditing protocol”.

This said, it is my understanding from the initial letter received from YHSSA with respect to this complaint, that there is no regular auditing protocol nor are there yet any policies in place with respect to the auditing of the EMR. Regular auditing may well have a significant deterrent effect on employees, but only if regular audits are actually done and there are follow ups done on any unusual activities that the audit uncovers. Having a “robust audit functionality” is only an asset if it is effectively used.

What the Report does not address in any fashion is the “role based” access to the system and how those roles were defined or whether they are being refined as the use of the system demonstrates situations in which the access is either too much or too little. In the words of Gary Dickson, the Information and Privacy Commissioner of Saskatchewan, “Role based access presents a huge challenge”. As we move from paper records in a small medical office where, perhaps, 5 or 10 people might be able to snoop in a file, to a system which connects, in the case of WOLF, some 150 people

and eventually potentially thousands of people across the Territory, how do you mitigate the risks with role based access? I can think of a lot of specific steps that might be taken in this regard:

a) thorough, comprehensive, consistent mandatory training for new employees about access to and the privacy of personal health information which consists of more than sitting down with a department head to chat about privacy issues as well as ongoing, regular in service training;

b) the preparation of comprehensive manuals detailing the rules for the collection, use, disclosure, access to and amendment of personal health information;

c) rigorous accreditation, including solid training and clear expectations of those who approve access to the system and give user privileges;

d) an ongoing auditing program of user activity by officials close enough to the point of service to be able to make the audit useful

e) clear and comprehensive policies that make a breach a serious matter that may warrant termination for cause;

f) a commitment from health profession regulatory bodies that they will take appropriate disciplinary action if their members improperly breach the privacy of patients;

From what I can gather with respect to WOLF, none of this work appears to have been done. In my estimation, YHSSA has a lot of work to do to hone the system, implement appropriate policies and procedures and to educate not only their own employees, but also the public as to how the electronic health record works.

Disclosure

The Report points out that there are times when medical or counseling information needs to be disclosed, either with the consent of the patient or by operation of law. In those situations in which YHSSA feels that express consent is necessary, there appear to be good policies in place, with the necessity of obtaining written consent from the patient and a requirement to put a note on the EMR that the consent was obtained.

The only exception to the practice of obtaining a written consent is in regard to continuity of care as, for example, when a patient is referred to a specialist. YHSSA considers this to be within the "circle of care" and that consent to this kind of disclosure is, therefore, implied. I would prefer to relate it to the actual wording of the *Access to Information and Protection of Privacy Act*. In cases where personal health information is disclosed to a specialist, and the patient has consented to seeing the specialist, the information disclosed is being disclosed for a purpose consistent with the purpose it was originally collected or is being disclosed with the implicit consent of the patient and the Act, in such cases, allows disclosure.

There are a number of instances in which the law requires disclosure of medical information, regardless of the views of the client. YHSSA has designated one person to address these situations and that person has ready access to legal support. These situations include:

a) where a search warrant or subpeona is presented;
b) in child protections matters;
c) vital statistics laws;
d) public health legislation

In circumstances where there is a legislated duty to report certain information, employees of YHSSA will do so. The Report, in fact, acknowledges that:

> It is fair to state that one of the primary reporting sources in public health and child protection is health care providers.

YHSSA will also disclose personal health information where there is a foreseeable danger to the health or safety of another individual.

All of these exceptions are specifically provided for in Section 48 of the *Access to Information and Protection of Privacy Act*, which provides that

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;

.....

(n) for the purpose of complying with a subpoena or warrant issued or an order made by a court, person or body that has the authority to compel the production of information or with a rule of court that relates to the production of information;

.....

(p) for the purpose of complying with a law of the Northwest Territories or Canada or with a treaty, written agreement or arrangement made under a law of the Northwest Territories or Canada;

(q) when necessary to protect the mental or physical health or safety of any individual

In these situations, the existing law allows for the further disclosure of personal information and it would appear that YKHSSA has a fairly good handle on when these circumstances exist.

<u>Other Issues in Privacy and Confidentiality and EMR's</u>

A. Secondary Uses of Information

The Report lists a number of secondary uses of the personal health information within the EMR, including:

- Research
- Improving Client Care; and
- Accountability

According to the Report:

> The EMR system has great capacity to be used as a research tool (ie. determining cancer rates, diabetes rates, etc.)

The Report acknowledges that secondary uses, including research, must be approached carefully. It refers to an excerpt from a paper prepared by the Canadian Medical Protective Association in 2008:

> Where it is intended that patient information will be used for purposes other than providing health care, great care must be exercised to ensure that there is express legislative authority for this secondary use or that the patient has consented to using his/her information for this other purpose. While some secondary uses, such as health system planning, are worthy objectives and form an important benefit of EHR's, patient confidentiality must always be protected. To the extent possible, patient information should be anonymized before it is used for purposes other than the provision of health care.[8]

That said, the Report also states that the EMR is an "exceedingly powerful" research tool and confirms that since the EMR has been running for a period of time, YHSSA is starting to receive requests for research that would not have been possible in the past.

Dr. Cavoukian and Mr. Alvarez, in a recent publication about secondary uses of personal health information in an electronic age, acknowledge the importance of these secondary uses of information, while cautioning against the inappropriate use of such information:

> It is also apparent that while the health sector is abundantly aware of the

---

[8] Electronic Health Records: A medical liability perspective http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com

> need for secondary use of the EHR, ordinary Canadians are not as familiar with the concept. In order to ensure the continued availability of complete and accurate EHR data for secondary purposes, it is important to maintain public trust in the EHR. In order to do this, we must address the potential challenges to privacy and confidentiality that are commonly associated with increasing secondary uses.[9]

The Report prepared by YHSSA points out that Section 49 of the ATIPP Act allows for the use and/or disclosure of personal information for research purposes in certain circumstances. It suggests that when the information is used for research, individual identifying information must be removed "as possible". In fact, the *Access to Information and Protection of Privacy Act* and the regulations under that Act provide for very strict rules which must be adhered to before any personal information can be disclosed for research purposes, including a requirement for a written agreement with the researcher which contains a number of very strict and very precise limitations with respect to the use and/or further disclosure of the information disclosed.

The Report suggests that the information which is contained within the WOLF system can also be utilized to improve client care (for example, monitoring to ensure that all diabetics have a hemoglobin AIC level check every three months and setting target blood sugar levels for the diabetic client group as a whole).

Further, the information in the EMR can be used to "improve efficiencies". For example, the Report suggests that WOLF can generate a list of a physician's diabetic clients and assign a staff member to make sure that hemoglobin AIC are up to date and completed for the client group, saving the physician the time of having to review individual charts. This continuity of care, they say, could result in fewer diabetes related illnesses, and fewer visits to the clinics and emergency room, resulting in significant

---

[9] *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

cost saving benefits.

There is absolutely no doubt that the EMR has huge potential for greater efficiencies and huge potential savings to the health system as a whole. That is clear and undisputed. The question is in how all of these things are accomplished while maintaining the privacy and the confidence of patients. Why, for instance, is it not possible to explain to diabetic patients that the EMR will produce regular reports to the physician which the physician or the clinic will then use to do follow up? This is the sort of thing that I think the ordinary person might even consider to be within the "circle of care" within which consent might be implied, particularly where they have been given notice that it will be happening. On the other hand, it may not be reasonable to imply consent to use the information in the EMR to "flag clients over 50 years of age to ensure that they all have bone density scans completed every two years", which was another example provided in the Report as a potential positive use of the information in the EMR.

If a patient is in a group that is going to be "flagged" it seems to me that they should be made aware of that potential. Most would likely acknowledge such services as a positive thing and thank YHSSA for it's thorough and efficient care. From that point on, consent to that use could be implied. Not before. I return to the fact that the current law allows use of personal information only for the use it was originally collected or a purpose consistent with that purpose and the "consistency" must be measured from the point of view of the patient, not YHSSA or the limitations of the EMR. Where there is doubt as to whether or not a use is "consistent" it would be my opinion, based on the general privacy provisions in the Act, that the benefit of the doubt should go to non-use or disclosure.

The Report does not confirm whether or not the information in the EMR is currently being used for research purposes. If it is, I would ask whether there are any policies or procedures in place to deal with requests for information for research purposes. Are there guidelines for when YHSSA might allow access to the information in the system to

a researcher in a format in which the individual patients can be identified? Most pure research can be done without identifiable data and I would suggest that there should be some level of proof required from researchers that identifiable information is required before YHSSA should even consider the disclosure of identifiable personal health information. Even if that proof were provided, I would suggest that there should also be some written policies in place which provide criteria which must be met before such information is disclosed and that there be only very limited and specific situations in which identifiable information is disclosed for research purposes without a client's explicit consent.

Again quoting from the recent report authored by Dr. Cavoukian and Mr. Alvarez:

> While identifiable information is clearly necessary in the context of delivering health care to individuals, personal health information is often not needed for secondary purposes – that should be the default. Therefore, personal health information should be routinely de-identified before it is used or disclosed for such purposes. To the extent that de-identified information may be used for a secondary purpose, privacy risks will be significantly minimized. The transition to EHRs presents new opportunities to build de-identification directly into processes and systems, consistent with PbD.(Privacy by Design) [10]

I have been left to wonder whether the WOLF system actually has the ability to anonymize personal health information for research purposes. In light of the other apparent limitations of the WOLF system discussed above, I would be surprised if this were the case. Unless and until this system clearly has that functionality, research should be relegated to a back seat.

---

[10] *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win* , Dr. Ann Cavoukian and Richard C. Alvarez, March 2, 2012, p. 6

CONCLUSIONS

Let me first say that I believe that those responsible for the privacy of personal health information within YHSSA are genuine in their desire to ensure that patients not only receive the best health care, but that they are also confident that their personal health information is secure and protected. That said, the people of Yellowknife no longer have a choice when it comes to primary health care. Other than the hospital emergency room, there really are only two options available in the City and the staff of those two offices rotates between the two clinics. There has been virtually no public education about either the benefits or the risks of the EMR. Nothing is said to patients when they book appointments or see their doctor to suggest that anyone other than a very narrow group of people will have access to any personal health information. I raised concerns even before the two new primary health clinics opened. In Review Recommendation #10-089, which involved an inappropriate disclosure of a patient's personal health information to his employer without his consent, I made the following comments:

> The issue raised in this review is timely. I understand that in the next month or two, all but one clinic in Yellowknife currently run by YHSS will be rolled into one "super clinic" with everything from family counseling to specialist services being provided under one roof. I am assuming that thought and care has been put into how patient files will be handled in this super clinic. The facts and circumstances of this case will, I hope, serve to focus some attention on these issues before the clinic opens, rather than after something like this happens again. Patients attending at the super clinic should be able to have confidence that their personal health records will not be generally available to anyone who works in any role within the clinic. Information collected and maintained should be compartmentalized and kept narrowly accessible and used only for the purpose for which it was collected and require the informed consent of the patient to have it accessible for another purpose, even if it is being used

> within the same physical space. Failure to do this will result in more complaints such as this one and will eventually lead to a loss of confidence in the system to the point that patients may choose to avoid seeing a doctor rather than to risk having their personal health information made widely available without their knowledge or consent.[11]

In 2010, Paul Fraser, the Acting Information and Privacy Commissioner for British Columbia undertook a review of the electronic health information system at the Vancouver Coastal Health Authority known as the Primary Access Regional Information System. In Investigation Report F10-02 he described the system as follows:

> The electronic health record system at Vancouver Coastal Health Authority ("VCH") known as the Primary Access Regional Information System ("PARIS") was introduced in 2001 for its community-based programs. It is accessed by staff and contractors involved in the delivery of a wide range of health services outside of acute care hospitals. These health services include such things as a newborn hotline, home support for seniors, detox services, and communicable disease control. The personal information contained in PARIS is highly sensitive. It includes diagnoses as well as the case notes of physicians, nurses and counselors about the treatment they provide to their clients.[12]

The investigation report found "major deficiencies in implementation of the PARIS software from a privacy perspective", including an access model that is team-based rather than role-based resulting in too many users having access to too much personal information.

> We found that the current model of access to other modules, including

---

[11] Northwest Territories (Public Body) (Re), 2010 CanLII 78802 (NWT IPC)

[12] CanLII Cite: 2010 BCIPC 13, pg 2

diagnosis and case notes, is:

- Team-based rather than role-based;
- Teams are multi-disciplinary health care teams which may be comprised of physicians, nursing staff, physical therapists, occupational therapists, counsellors and administrative support staff
- Almost all team members have access to the same personal information
- Team directors can authorize access or removal

This team-based or workgroup-based access control permits too many users to have access to too much personal information. It is not sufficiently granular and does not adequately reflect the need-to-know and least privilege principles.[13]

This appears to be the approach being taken by YHSSA in it's two primary care clinics.

Based on what I have discovered while doing this report, I would express the following concerns and raise the following issues:

1. As predicted in my Recommendation #10-089, it appears that personal health information is not being compartmentalized but instead is being made generally available through all "departments" within the two major clinics and, in fact, between the two clinics in light of the fact that the staff rotates between them. As a result, there are far more people within the system who have some degree of access to much more of an individual's personal health information. Moreover, the public is unaware of how their information is being used and shared.

---

[13] CanLII Cite: 2010 BCIPC 13, pg 23,24

2. The public body did not provide me with any detailed analysis about how the "roles" which govern the role-based access to the system were created. Based on the information that I do have, however, it would appear that the roles have been defined so as to allow access to as much information as possible to as many people within the system as possible. In my opinion, and keeping in mind the discussion above, it is my opinion that roles should be defined as narrowly as possible to restrict access to as much information as possible to the fewest number of people in the system without substantially reducing the level of care provided. As other Canadian jurisdictions have discovered, role-based access makes sense in the abstract, but the roles are not so easy to define in practice. As noted by my colleague, Gary Dickson, of Saskatchewan, the definitions need to be developed with "granularity" in mind. Furthermore, there needs to be ongoing monitoring of the effectiveness of the definitions used for each level of "role based" access to the system. The roles need to be reviewed and adjusted over time as use of the system helps to define when certain "roles" really do not need certain information and when, perhaps, other roles might need more. There may be a real need to expand the number of roles so as to effectively limit unnecessary access to the EMR. Certainly, the definition of "roles" and the level of access attached to those roles will, in the long run, be pivotal to the success of any EMR.

3. Having reviewed all of the materials provided to me, it appears that, at least to some extent, the technology is driving the solutions, rather than the other way around. YHSSA needs to make the technology respond to the needs of the system and to find the technology that will address the problems, rather than to hobble together solutions based on the limitations of the technology.

4. A lot more work needs to be done to ensure that both the public and YHSSA fully understand both the benefits and risks inherent in an EMR. I am convinced that most people would be absolutely appalled to know that some level of counseling

records are unavoidably available to 143 people who work within the system. As noted by YHSSA in their Report, Yellowknife is a small town and inevitably at least one of those 143 people is going to have some connection to each patient who walks in the door, whether as a friend or a relative or a friend of a friend or relative. I also think that there would be significant repercussions if a patient struggling with personal issues knew that the Director of Social Programs has authorization to access counseling records, whether or not that authorization is ever actually used to gain access. The Director of Social Programs is an individual whose job it is to intervene in homes where there are personal issues. We absolutely do not want people choosing not to seek counseling for fear that the Director of Social Programs might swoop in and apprehend children after seeing personal health information.

5. It is clear to me that the concept of "circle of care" needs to be defined and in my opinion, that definition should be created from the perspective of the patient, and within the limitations of the ATIPP Act, and not from the perspective of the efficiency of the system. As my colleague, Gary Dickson of Saskatchewan so eloquently stated in the Postscript to his Investigation Report - 2010-001:[14]

> The development of an EHR requires a complex balancing of a number of competing goals or values. Obviously the success of any iEHR initiative will require the cooperation and full participation by Saskatchewan health care professionals. There are many examples of features of the iEHR plan in Saskatchewan designed to address the convenience of those professionals. It is also true that while privacy of Saskatchewan residents is important it is not an absolute right and from time to time may be limited to accommodate certain legal requirements, safety requirements and public policy initiatives. The challenge is to find a way of balancing

[14] Saskatchewan Investigation Report H-2010-001, Postscript, Information and Privacy Commissioner of Saskatchewan, March 23, 2010, p. 53

those values which may from time to time be in conflict. In my view, the evident preoccupation with making the iEHR simpler for health care professionals - the providers - has to a large degree eclipsed the need to make our iEHR sufficiently respectful of the expectations and rights of the patient. This preoccupation with accommodating the preferences as well as the needs of providers perhaps accounts for some of the vulnerabilities exposed in this investigation. Fortunately, our iEHR is still a work in progress. There is still the opportunity to recalibrate - to implement stronger controls and safeguards to better protect the interests of the patient. I think such action is consistent with the thrust and recommendations of Commissioner Dagnone in his *Patient First Review Report* and specifically the following observation:

> Fundamental to achieving patient - and family - centred care is patient-centered governance and policy-setting, beginning with the Ministry of Health and supported by unified, prudently managed, high-performing health care administration that enables, empowers and expects everyone to put the patient first.[15]

It appears that all information currently gathered by YHSSA is considered to be usable for pretty much any medical issue within the Authority, regardless of why it was originally collected, unless the patient specifically requests that there be limitations put on that use. In their initial letter to me, YHSSA made the following statement:

> Secondly, as a Health and Social Services Authority, there are basic principals that guide the way we manage and share information. Unless precluded by legislation to the contrary, as in

[15] Saskatchewan Health, *For Patient's Sake: Patient First Review Commissioner's Report to the Saskatchewan Minister of Health,* available online at www.health.gov.sk.ca/patient-first-review, p. 12

> the case of child protection legislation, we as a Health Authority, can share client information within the Authority as needed to facilitate our functions without client consent.

What seems to be missing here is an understanding that the *Access to Information and Protection of Privacy Act* **does** preclude such widespread sharing of information in their system. There appears to be a reliance on an overly wide interpretation of "consistent purpose" so as to impute an implied consent to any and all uses of personal health information within the Authority. To me, this is disrespectful of the patient and very difficult to reconcile with a patient centered approach or the terminology contained in the ATIPP Act. This issue, above all, must be addressed. It comes back to the concept of informational privacy as defined by the Supreme Court of Canada in *R. v. Duarte* and quoted in the Report prepared by YHSSA for this review. To repeat the statement made earlier in this report, the Supreme Court held that informational privacy is:

> "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself".[16]

In my opinion, YHSSA needs to re-think the limitations of the implied consent, particularly in light of the very wide range of services available in each of the two clinics and the lack of an educated public. I strongly recommend that, at least until such time as the public is better educated about the system, YHSSA find ways to protect personal health information "between departments" such that information collected for the purpose of mending the broken leg, for instance, is not available to the people engaged in counseling services.

---

[16] [1990] 1 S.C.R. 30 at 46

6. As a corollary to this, I am concerned that WOLF appears to offer only an “all or nothing” approach to the masking of information. Either electronic medical information is available to everyone in the system (subject to their roles) or it is available only to the author. There is no “in between” and there is no option available that would allow only one or two people to be prohibited from accessing a patient record. As other jurisdictions have discovered, it is the curious employee who is most often the cause of a wrongful use or disclosure of personal information. An ex spouse who wants to find out what’s going on the life of his former partner or a curious neighbor who wants to know what happened next door, or the family friend who just wants to make sure that everything is okay with his/her friend. In a small community like ours, this is going to come up more often than it might elsewhere. There has to be some function which allows the system to “lock out” certain individuals from certain files. Not only must the system have that functionality, the public has to be aware that the “lock outs” are possible so that they know to ask for them. I am aware that if too many people elect to ask for such lock outs, it will affect the efficiency of the system. This is the only way, however, to give the individual the “right to determine for himself when, how and to what extent” his personal health information can be used.

7. I am concerned that it appears that, more than a year after the launch of the EMR in the two Yellowknife clinics, there is either no auditing being done, or that the auditing being done is minimal and without any underlying protocols or policies in place. It does no good whatsoever to have auditing capabilities if they aren’t being used, or aren’t being used in a manner that will provide disincentives to improper “peeking” or flag abnormalities. Then again, in order to catch an abnormality, there has to be some measure of what constitutes an abnormality. Having audit functions available within the system are of little help unless they are used effectively to ensure that the security of the system is maintained.

In summary, a lot of work is required to bring the EMR in line with our legislation. Efficiency is important, but not transcendent. The most efficient system would be one where patient personal health information flows easily without any walls or barriers of any kind. Such a system, however efficient, would not be trusted by patients. Already with paper records there are studies which identify approximately 12% of patients who withhold information even from their primary health care providers for a variety of personal reasons. A system with no privacy protections, or even faulty privacy protections, would result in even higher levels of mistrust and reticence to either obtain needed medical intervention or reveal all of the relevant and important information needed to treat the patient. Privacy is a fundamental value and the right of all Canadians, protected by the Charter of Rights. The EMR system being developed must conform to privacy best practices. Based on what I have learned through this review, there appears to be a need to return to basics and to "recalibrate" the system so that it is more respectful of the rights of individuals to control how, when and to what extent their personal health information is being used. To that end, therefore, I make the following specific recommendations with a view to improving the EMR to ensure that it works to allow better integration of services while at the same time allowing the individual the right to control access to his/her most sensitive of personal information.

Recommendation #1

Although YHSSA has no ability whatsoever to control the preparation or tabling of health specific privacy legislation, it is clear that such legislation is required to address some of the issues raised in this report. My first recommendation, therefore, is directed to the Department of Health and Social Services, rather than to YHSSA and that is to do what is necessary to make the tabling of health specific privacy legislation a priority. I am aware that the Department has been working on such legislation for a number of years but it does not appear that this work has been progressing quickly. This legislation is essential to deal with the nuances of personal health information and how it is handled. That said, it is important as well that the legislation recognize the right of

the individual to informational privacy, as defined by the Supreme Court of Canada and enshrined as a right in the Charter of Rights.

Recommendation #2

I recommend that YHSSA immediately find ways, working with the software developer, to improve WOLF so that it meets the needs of the system, rather than it limiting it. Specifically, WOLF needs to be able to

a) "lock out" one or more users from specific health records;

b) have sufficient granularity within the defined "roles" so as to allow it to create silos of information so that patients can be satisfied that information gathered for one purpose is not being used for another purpose;

c) have the capacity to limit access to information in a fashion that truly reflects the employee's "need to know" and the functions of his role. This may well require the addition of more "roles" within the system.

Recommendation #3

I recommend that the public body create comprehensive policies detailing the rules for the collection, use, disclosure, access to and amendment of personal health information. Central to these policies should be a definition of "circle of care" that would accord with the "reasonable person's" understanding of that term and the requirements of the *Access to Information and Protection of Privacy Act*.

Recommendation #4

I recommend that YKHSS do a complete review of the definition of the “roles” within the system and that careful attention be given to which individuals really need to have access to which information in order to provide good medical health services. Do counselors need or want prescription information? Do x-ray technicians really need to know that a patient is in counseling? Does a clerk making an appointment really need to have a list of previous treatments on the screen to make an appointment for a patient? The “need to know” must always, always be respectful of the patient’s right to determine for himself when, how and to what extent he his medical health information is being used.

Recommendation #5

I recommend that all employees be given standardized and consistent training when commencing employment with YHSSA with respect to ATIPPA, confidentiality, security and privacy of personal health information, including warnings with respect to consequences (including dismissal) for failing to comply with the standards set. Furthermore, I recommend that there be mandatory regular, in-service training on these issues, for each employee at least once every two years.

Recommendation #6

Priority must be given to implementing an ongoing auditing program of user activity by officials close enough to the point of service to be able to make the audit useful. Audits should be done on a regular basis and staff should be made aware that such audits are done regularly so as to dissuade employees from inappropriate snooping.

Recommendation #7

I recommend that YHSSA create a comprehensive and easy to understand educational campaign to educate the public about both the benefits and risks of the EMR, and that steps be taken to ensure that patients are made aware of what their personal health information will be used for and that they be provided with the tools they need to decide for themselves how much or how little information they are comfortable with being available generally to all employees of YHSSA.

Recommendation #8

I recommend that there be serious consideration given to whether or not it is appropriate for the Director of Social Programs to have access to the personal health information of individuals seeking medical attention at either of the primary health clinics. It is my recommendation that there be no such access. As noted in my discussion above, people in Yellowknife have no choice in terms of choosing a family doctor or a primary care physician than to go to one of the two clinics. There has been no explanation given to me as to why the Director of Social Programs would require access to personal health information. Nor was I advised where the Director stands in terms of what access he/she has to the system (full access/partial access). This is not someone who is in any way within the "circle of medical care" no matter how widely that circle is drawn. I am very concerned that those who need help most would avoid seeking that help if they were aware that the Director of Social Programs had access to their personal health information, counseling records, and the like.

These recommendations have to be taken as a "starting point" for ensuring that WOLF complies with the legislative provisions in the *Access to Information and Protection of Privacy Act*. They are not comprehensive or detailed. Electronic medical records are, without any shadow of a doubt, a positive development in the provision of medical care. The concern is that, unless YHSSA can assure the public that their information is being used, viewed and disclosed in a way that respects their personal privacy, the

anticipated benefits of the system will quickly disappear because of a reluctance to open up sensitive medical information to the prying eyes of a large number of employees. The fact that the two clinics in Yellowknife represent the only recourse for primary health means that extra care must be taken to ensure privacy.

Elaine Keenan Bengts
Northwest Territories Information and Privacy Commissioner