TABLE OF CONTENTS

PRIVACY AUDIT REPORT
QIKIQTANI GENERAL HOSPITAL

INTRODUCTION

After my last appearance before the Standing Committee on Oversight of Government Operations and Public Accounts the Committee recommended that my office undertake a privacy audit of a major government institution in Nunavut. In response, I decided to undertake an audit of the Qikiqtani General Hospital (QGH).

The reasons why I chose the QGH for my first privacy audit include:

- QGH is one the largest employers and one of the most important service providers in Nunavut
- Personal health information is one of the most sensitive and prejudicial types of personal information of residents in Nunavut. The largest concentration of such PHI would presumably be in the custody or under the control of QGH and the GN Department of Health.
- The implementation of electronic medical records such as the Meditech system in the QGH create not only benefits for patients and providers but also create some significant new privacy challenges
- The paucity of formal complaints relating to the QGH in contrast with most other government institutions raised concern that the transparency obligations were not being adequately met and discharged. In my office's experience that may indicate patients are not made aware of their privacy rights and the remedies available to them for breach of privacy.

The QGH is an acute care hospital located in Iqaluit, Nunavut. It has approximately 35 beds, although only 22 are currently open. There are no long term care beds and those patients are sent to Ottawa. It is the only acute care facility in the geographically large territory which serves approximately 32,000 residents. It has approximately 150 employees including physicians, nurses, other health professionals and support staff. All of these employees are employees of the GN.

QGH has the following departments:

Health records

Diagnostic Imaging

Operating rooms

In patient care

Clinics

Pharmacy

Laboratory

Emergency room

Information Technology (IT)

QGH also has written agreements with the Ottawa Hospital to facilitate the transfer of patients for health services not readily available in Iqaluit. About one quarter of the Department of Health budget is spent on medical travel and treatment provided at out of territory facilities.

Although QGH is the only hospital in Nunavut, the territory also has new regional facilities in Rankin Inlet and Cambridge Bay with in and out-patient capacity and 24 local health centres.

There is an interesting relationship between QGH and the Department of Health (formerly Health and Social Services). The QGH is not a "public body" for purposes of ATIPPA. It is not a "department, branch or office" of the GN as required by s. 2(a) of ATIPPA. Nor is it an "agency, board, commission, corporation, office or other body designated in the regulations".

It is the Department of Health that is the public body with responsibility for QGH. In fact, all employees of the QGH are employees of the GN. The contracts outsourcing certain medical specialist services are with the Department and not the QGH. Although the focus of this audit is the QGH, it has been necessary to also consider certain practices and arrangements with the Department when they directly impact privacy in QGH.

When we requested copies of privacy policies in force in QGH, we were provided not only with documents bearing the Qikiqtani General Hospital name but also a number of documents bearing the Nunavut Department of Health name (or Health and Social Services as it was previously named). At the outset of our audit, we notified the Department of Health's Director of Policy in order to share the plan for the audit. During the audit we had discussions with the ATIPP coordinator for the Department of Health. Subsequent to our hospital tour we were able to speak with the Assistant Deputy Minister for Health and former Director of Policy in the same department.

I wish to acknowledge and thank the Director of Clinical Services at QGH and the ATIPP Manager for the GN for the excellent cooperation and assistance received from these individuals both in preparation for the audit and then throughout the completion of the audit. Both of these individuals demonstrated a strong commitment to vigorous privacy protection of Nunavut patients and a refreshing willingness to consider improvements to policy, practices and procedures.

AUTHORITY

The Office of the Information and Privacy Commissioner of Nunavut has been created pursuant to section 61 of the ATIPPA. The powers of the Commissioner are delineated in ATIPPA including section 67 that provides as follows:

> 67. The Information and Privacy Commissioner may
>
> a) engage in or commission research into matters affecting the carrying out of the purposes of this Act;
>
> b) receive representations about the operation of this Act; and
>
> c) offer comment on the implications for privacy protection of proposed legislative schemes or government programs.

In terms of reviewing the collection, use or disclosure of personal information of any individual by a public body such a review can be triggered either by a request from an individual (s. 49.1(1)) or where the Commissioner "has reason to believe that a public body has or may have collected, used or disclosed personal information in contravention of this Act", in which case the Commissioner "may review the practices of

the public body with respect to the collection, use and disclosure of personal information". (s. 49.1(2))

Section 49.2 provides as follows:

> 49.2(1) The Information and Privacy Commissioner may conduct a review under section 49.1 if he or she is of the opinion that a review is warranted in the circumstances.

The head of the public body must be given an opportunity to make representations to the Information and Privacy Commissioner doing the review.

By reason of s. 49.5 "On completing a review , the Information and Privacy Commissioner shall (a) prepare a written report setting out the recommendations of the Information and Privacy Commissioner with respect to the collection, use or disclosure of the individual's personal information and the reasons for the recommendations; and (b) provide a copy of the report to the … head of the public body concerned."

S. 65(1) authorizes the Commissioner to "employ or engage the services of any persons necessary to assist in carrying out the duties and functions of the Information and Privacy Commissioner." I exercised this authority to contract with a consultant with expertise in the area of health information and privacy to assist with the planning and execution of the audit plan.

In addition to the relevant statutory obligations, the extensive experience in Canadian provinces and territories with health information, privacy, electronic medical records and electronic health records has led to the identification of a number of privacy best practices. For purposes of this audit, I was were guided by the guidelines produced by the Canadian Health Informatics Association (COACH). Of particular value are the *2013 Guidelines for the Protection of Health Information* (www.coachorg.com) and the *2013 Putting It into Practice, Privacy and Security for Healthcare Providers Implementing Electronic Medical Records, Special Edition* (www.coachorg.com).

PROCESS

By a letter dated February 24, 2016 I notified the QGH of my intention to undertake an investigation of the collection, use and disclosure practices of the institution. I indicated that this would take the form of an audit. A formal Audit Plan was developed through

subsequent discussions with the QGH. This included a March 18, 2016 conference call with the Director of Operations at the QGH and the Director of Policy for the Health Department GN. Subsequently, the Audit Plan was approved and signed by the Director of Operations on behalf of the QGH.

The OIPC requested and obtained from QGH current organization charts depicting the distribution of authority to make decisions about privacy compliance and as well copies of any privacy policies or procedures then in use in QGH.

QGH provided 44 documents which are particularized on Schedule 1. This included three policies of QGH (Disclosure of Harm, E-mail consultation and Confidentiality), one Department of Health Mailing Log Sheet and the Directive: Sending and Receiving Confidential Email and Mail, Policy #A-001, three from Executive and Intergovernmental Affairs (Social Media Policy, Privacy Breach and Incident Policy, Access to Information and Privacy Policy), one from the Department of Community and Government Services (Acceptable Email & Internet Usage Policy and Records Management Policy) , and one from the Department of Culture, Language, Elders and Youth (Archives Policy).

My office attended at QGH from June 6, 2016 to June 9, 2016 for meetings and a tour of the hospital. This included inspecting the facilities for the following services:

- Reception and admitting
- Diagnostic Imaging
- Health Records
- Clinics
- Operating Room
- Emergency
- Pharmacy
- In patient care

On June 6, 2016 the OIPC commenced our four day on-site tour of the facility with a meeting with the directors and heads of the various departments in QGH organized by the Director of Operations. This was in preparation for our individual meetings with those directors and heads of departments. This involved an explanation of the investigation/audit, the types of information we would be seeking and the purpose of the

resulting report. We advised these officials that we would be doing thorough fact-checking and would make the draft report available to the leadership of QGH and the Department of Health before it was finalized.

In addition, during the time in Iqaluit we also met with the ATIPP coordinator for the GN Department of Health and the Manager of ATIPP for the GN.

Near the conclusion of our on-site interviews at QGH, we learned of a Privacy Impact Assessment (PIA) that had been done years earlier and a suite of policies ostensibly to enable an electronic health record in Nunavut. We then obtained copies of those documents and subsequently reviewed same. Those documents are particularized on Schedule 2.

ON-SITE, IN-PERSON INTERVIEWS

During the time in Iqaluit, we met with the following officials:

- Director of Operations
- Acting Manager of Health Records
- Director of Health Records
- Acting Director of IT
- Clinics Nurse Manager
- Inpatient Care Nurse Manager
- Emergency Nurse Manager
- Contract Pharmacist at Ottawa General Hospital
- Operating Room Manager
- Clinical Nurse Educator
- Diagnostic Imagining Director
- Department of Health ATIPP Coordinator
- GN ATIPP Manager

In addition, we had subsequent telephone interviews with:

- Laboratory Manager
- Assistant Deputy Minister, Department

FINDINGS

THE APPROPRIATE "PUBLIC BODY" FOR PURPOSES OF ATIPPA

As noted earlier, it is the Department of Health that is the "public body" responsible for purposes of ATIPPA with all of the collection, use and disclosure of personal health information within the QGH. That may have been sensible before the advent of electronic medical records and electronic health records. With the development of new clinical information systems that aggregate large volumes of sensitive personal health information on many residents it perhaps should be reconsidered. It may be that this current arrangement contributes to the lack of privacy leadership in QGH identified and discussed in this Audit Report.

The QGH is one of the larger public sector organizations in Nunavut. Unlike other GN departments, it is unique in providing direct medical services to individuals. In QGH there is a need for the collection, use and disclosure of large volumes of personal health information of those individuals. Perhaps unique among government services, there is a long standing culture of confidentiality for the delivery of health care services. This is reinforced by the training of clinical professionals and by codes of ethics and standard healthcare procedures. The Department of Health, under which QGH is currently subsumed for purposes of ATIPPA, has all kinds of administrative responsibilities for the provision of health care services to Nunavummiut. The Department is not normally engaged in the diagnosis, treatment and care of individuals but rather in providing and supporting the infrastructure to ensure those services are available. In considering the more than 25 years of Canadian experience with electronic health information systems, it appears that the more distant the seat of responsibility for statutory compliance is from the point of service, the less robust the privacy regime is likely to be. In terms of ensuring appropriate accountability for the collection, use and disclosure of personal health information, I recommend that QGH and, in fact, all health facilities in Nunavut be designated as separate "public bodies" for purposes of ATIPPA.

This would mean that the Executive Director of the QGH would be the "head" under ATIPPA and answerable for what is done with the personal health information of patients in QGH. At some point, once there is fully functional and mature electronic health record system, it may be appropriate to reconsider accountability to the patient and how that can best be ensured.

This recommendation, if implemented, would mean that QGH is treated in an equivalent way to the Arctic College, the Nunavut Housing Corporation or the Business Credit Corporation and other bodies designated in Schedule A of the ATIPPA Regulation as a "public body".

Recommendation:

That the QGH and all other health facilities be designated in the ATIPPA Regulation as "public bodies".

IS THE ATIPPA THE 'BEST FIT' FOR ELECTRONIC HEALTH RECORDS?

As noted above, the applicable law for purposes of this Privacy Audit is the *Access to Information and Protection of Privacy Act*. This is a law of general application similar to access and privacy laws in all Canadian provinces and territories. It is in effect two laws in one. Part I provides a code for access to information and Part 2 provides a code for the protection of privacy. Such a law applies to government institutions only. As with other provincial and territorial access and privacy laws, ATIPPA reflects a scheme first outlined in the 1980 Royal Commission Report on Freedom of Information and Individual Privacy from Ontario. The explicit purpose of such a law was to improve public information policies and relevant legislation and procedures of government, while protecting the rights of individuals to personal privacy.

In the late1990's and early 2000's those provincial and territorial governments made decisions to move towards the development of electronic health records for their residents. These decisions were influenced by the work of the federal Advisory Council of Health Infostructure. Its 1999 report recommended that all jurisdictions create electronic health records to improve health outcomes, to facilitate health resource planning and health research. Fundamental to such recommendations was the need for jurisdictions to create a new set of rules to govern the collection, use and disclosure of personal health information (PHI). This was predicated on the realization that the

healthcare system, unlike any provincial/territorial government body, is dependent on extensive sharing of PHI among a large number of providers, institutions and bodies including pharmacists, diagnostic imaging clinics, hospitals, health ministries, public health agencies, physicians, nurses, physiotherapists, laboratories and many more. Electronic health records would involve both public sector organizations such as hospitals and health ministries but also private sector organizations such as pharmacies, laboratories and diagnostic clinics.

That led to the creation of stand-alone health information laws which would have two primary purposes: (1) to facilitate easy and timely sharing of PHI among health care providers with a legitimate need to know for clinical purposes or support of those services and (2) to prevent disclosure of that PHI to or use by other persons who would not have that legitimate need to know. The first was Manitoba's *Personal Health Information Act* in 1997. That was followed by Alberta's *Health Information Act* in 2001 and by *Saskatchewan's Health Information Protection Act* in 2003. Ontario's *Personal Health Information Protection Act* (PHIPA) came into force in 2004. To amend PHIPA, Bill 78, the *Electronic Personal Health Information Act* was tabled in May 2013 and awaits proclamation. New Brunswick's *Personal Health Information Privacy and Access Act* came into force in 2010. Newfoundland's *Personal Health Information Act*, SNL 2008, c. P-7.01, in 2011. The Northwest Territories *Health Information Act* came into force 2015. Nova Scotia's *Personal Health Information Act*, SNS 2010, c. 41 as amended, with Royal Assent May 2014 is awaiting proclamation, PEI's *Health Information Act* received Royal Assent May 2014 and awaits proclamation. The Yukon's *Health Information Privacy and Management Act*, S.Y. 2013, c. 16 was passed in 2013 and came into effect on August 31st, 2016. Quebec's *An Act respecting the sharing of certain health information* (2012, c. 23) has specific provisions for collection, use and disclosure of PHI in its public sector/private sector.

These various provincial laws reflect the Pan-Canadian Health Information Confidentiality and Privacy Framework created by provincial Ministers of Health in 2004. This was endorsed by all provinces save for Quebec and Saskatchewan.

Canada Health Infoway is the federal non-profit corporation funded by the Government of Canada to assist provinces construct their provincial components of what is ultimately to be a pan-Canadian interoperable system of electronic health records for every man, woman and child in Canada. See the Canada Health Infoway, Vision 2015-

Advancing Canada's next generation of healthcare. Toronto: Canada Health Infoway; 2010. Available: https://www.infoway-inforoute.ca/.

I note that in the August 1, 2013 Response to the Standing Committee on Oversight of Government Operations and Public Accounts' Report on the Review of the 2011-2012 Annual Report of the Information and Privacy Commissioner of Nunavut, the Standing Committee had requested an account in detail of the GN's "progress to date in addressing the issues of health-specific privacy legislation and the management and security of electronic health records". The Department of Health response was that, "The Department of Health will be reviewing health-specific privacy legislation in other jurisdictions. Based upon this review, it will consider how to move forward in this area. Nine privacy and security directives with respect to electronic health records have been completed, approved and implemented." In the course of this audit we determined that the review appears to have stalled and the nine privacy and security directives were not approved until June 2013 and none have been implemented. This is addressed elsewhere in this Audit Report.

British Columbia has to date not followed the model of a stand-alone health information law. That appears to be changing. The former B.C. Information and Privacy Commissioner had called for such a law in her *Prescription for Legislative Reform* of April 2014.

> The current legal framework to protect the data flows in the health sector has not kept pace with the new digital reality. B.C.'s current privacy laws of general application lack clarity and consistency and are not tailored to the unique nature of PHI and how it is managed in the health sector.
>
> …
>
> No one would argue with the need to protect personal health information. It is the most sensitive type of personal information because it is information about our body, our state of mind and our behaviour. As Information and Privacy Commissioner, I am concerned about how this sensitive personal health information is protected in privacy law and policy. I am convinced that new health information privacy law is needed in BC.
>
> Reform of the current complex and fragmented legislative framework is long overdue. The current legislation is inadequate in comparison to

> legislation in place in other provinces and is out of step with today's dynamic health sector.
>
> This report recommends new tailor-made legislation and policy that will protect the privacy of personal health information in a way that is comprehensive, consistent and forward-looking. It also needs to authorize data flows that are necessary for the efficient and cost-effective delivery of health services in BC and permit appropriate secondary use.
>
> While it is desirable for privacy and security frameworks to have legal force and effect, at the same time, they need to be agile. That is, flexibility needs to be built in so that the legislation is adaptable to new technologies and models of health service delivery.
>
> New health information privacy law needs to properly protect privacy and with the specificity, certainty and transparency that the public deserves. Given current legislative approaches to health information privacy elsewhere in Canada, and abroad, it would not be at all surprising if the government here in British Columbia decided to move forward with new health information privacy legislation. I urge government to move forward on such an initiative consistent with this Special Report and as a matter of high priority.

In the report to the Legislative Assembly from the Select Special Committee on the Personal Information Protection Act in British Columbia, the all-party committee had recommended as follows:

> Health Information Privacy Law
>
> The Committee received a submission from the Canadian Medical Protective Association that recommended, among other things, that government enact new stand-alone health information privacy law as exists in other jurisdictions in Canada. The Association said that it would provide an effective governance framework for the provincial electronic health record to ensure there is a balance between privacy and subsequent use of information through data analytics. A separate health information privacy statute would have implications regarding the scope of application of PIPA because PIPA applies to health professionals in

private practice. It would also carve out the Ministry of Health and health authorities from the scope of FIPPA.

In response to Committee questions, the Information and Privacy Commissioner advised that she is in favour of health-specific privacy legislation in BC because the health sector is unique and requires special consideration. She advised that she had issued a special report advocating such legislation in April 2014.

The Committee was of the view that the provincial government should develop a stand-alone health information privacy law that would govern how personal health information is collected, used, disclosed, and protected within the integrated health sector.

The Committee recommends that:

Recommendation

14. The provincial government develop a new health information privacy law that is consistent with laws in other jurisdictions in Canada.

I agree with the former British Columbia Commissioner and the Legislative Committee. I have no hesitation in recommending the same action in Nunavut.

Recommendation:

I recommend that the GN develop a stand-alone health information law similar to such laws in other Canadian jurisdictions. This would include a broad definition of personal health information, a clear definition of who would qualify as a custodian and appropriate rules for the collection, use and disclosure of personal health information. This should also include a statutory right of anyone to request access to their personal health information and the right to request that errors be corrected. The custodian should be subject to an explicit duty to assist applicants in exercising their right of access. The approach to consent should be one focussed on implied consent to align with the approach in other provinces. This would be subject to certain kinds of disclosure requiring express consent and for a limited number of purposes no consent required. I recommend that the Information and Privacy Commissioner be the oversight office to ensure that there is some consistency in the approach to privacy compliance overall in Nunavut.

Some of the other stand-alone health information laws are very dense and complex. My recommendation is that the focus should be on ensuring that the law is as straight-forward and accessible as possible. That should facilitate better understanding and ultimately higher levels of compliance at QGH.

NEED FOR A PRIVACY OFFICER

There is no Privacy Officer for QGH. This is perhaps the most significant gap among a number of gaps in terms of privacy protection in this important institution. What exists is confusion over what is required by employees, and in some cases their managers, in order to comply with ATIPPA and privacy best practices. In some cases, certain individuals may be contacted when staff have privacy questions but these individuals often do not have the training and experience and certainly don't have the mandate to provide direction to these staff members. Privacy law and practice is a fast changing environment which is affected by new technologies and new privacy challenges. It is a full-time job for a qualified professional to stay current with such changes.

In our interviews, the absence of a properly qualified and trained Privacy Officer was identified as a problem with privacy compliance. There was strong support from the managers/directors we met with for the creation of such a position. The need for a strong training program and leader is illustrated by the commentary of an Alberta Court of Appeal Justice who was considering a case involving the Alberta equivalent to the Nunavut *Access to Information and Protection of Privacy Act*:

> "…both FOIPPA and PIPA are complex pieces of legislation. Sections in each refer to other sections and when those sections are scrutinized they refer to yet more provisions. Each act is a web, or more accurately a maze, which make them difficult to interpret. Their enactment has resulted in an entire new area of law requiring specialists who traverse their intricacies. To suggest that they are user unfriendly is an understatement." Alberta (Information and Privacy Commissioner) v. Alberta (freedom of Information and Protection of Privacy Act Adjudicator), 2011 ABCA 36 at para 15.

Appendix C to the Privacy Framework for Protecting Personal Information in the Government of Nunavut iEHR is a job description for such a Privacy Officer. This is a good start but is deficient in the following respects:

- The individual should be senior in the QGH organization with ready access to the CEO and the management team of QGH.
- The individual should be responsible for dealing with patient privacy complaints and requests for access to PHI under either a stand-alone health information statute or ATIPPA.
- This should include responsibility to provide advice to the CEO and management team with respect to new programs, policies and procedures.
- This job description should explicitly address dealing with the Information and Privacy Commissioner on a regular basis.
- This individual should explicitly be charged with providing advice on privacy compliance to the regional health centres and to the Department of Health.

A CAUTION

There apparently has been some work done by the Nunavut Department of Health with respect to developing a job description for a Privacy Officer for the Department who would also serve as the Privacy Officer for the QGH. The position has never however been actually created and staffed. Mindful that there are fiscal limitations and a need to ensure efficiency and economy wherever possible in the delivery of public services, I question whether relying on a Privacy Officer for the Department of Health can provide the hands-on day to day leadership required in QGH. This is for a couple of reasons:

- QGH is the only acute care facility in Nunavut. It has a critical mass of healthcare workers, including nurses and physicians. The largest volume of health information transactions (collection, use and disclosure) in Nunavut presumably occur in QGH.
- The Department of Health is to some extent remote from the hospital and although it will be dealing with large volumes of PHI, this will not for the most part involve collection, use and disclosure for clinical or therapeutic purposes. The majority of challenging privacy issues involving PHI will occur in the context of clinical or therapeutic services.

- To house the health privacy leadership role in the Department deprives the QGH and its 150 employees and all of the patients it serves of the most robust possible privacy regime.
- There is no reason why the Privacy Officer in the QGH cannot also serve as the leader of health privacy throughout the territory while also fulfilling the role as privacy leader in the QGH.
- Privacy Officers improve their knowledge through practical experience available primarily in the acute care context because of the more intense type of PHI sharing. Assigning the role of privacy leadership to someone in the Department of Health minimizes the opportunity to gain that practical experience.

Recommendation:

I recommend that QGH appoint a Privacy Officer with the following features:

- **Designated leadership role to lead the privacy compliance efforts in QGH,**
- **Sufficiently senior to be able to have ready access to the CEO and senior management,**
- **Mandated to develop and implement a comprehensive privacy management program, to include privacy management within the Records Department of QGH,**
- **To provide input to the CEO and senior management on achieving good privacy compliance in new programs, new software and policies,**
- **To be responsible for developing a full suite of written policies and procedures for privacy compliance and to oversee staff privacy training for both the orientation of new hires and in-service training for existing employees as well as volunteers and contractors,**
- **To ensure proper privacy protection in out-sourcing contracts that involve significant volumes of personal health information,**
- **To be the key liaison between the QGH and the Office of the Information and Privacy Commissioner,**

- **To be closely associated with the Records Department and the IT department to ensure that privacy considerations are regularly and fully canvassed by those departments in the course of their work,**
- **To consider how to ensure that information about patient's privacy rights are brought to the attention of patients and the public by means of brochures, posters and the QGH website,**
- **To take steps to ensure that the QGH Quality Assurance Coordinator and that officer's work do not in any way interfere, obstruct or impair the role and focus on the Privacy Officer and the privacy rights of patients and members of the public. This would include at a minimum ensuring that the Coordinator receives appropriate privacy training and that there is clear communication between the Coordinator and the Privacy Officer.**

This audit clearly demonstrates the need for those clear and consistent rules to govern PHI whether in the public sector or the private sector in Nunavut if Nunavut is to conform to best practices across Canada.

ORGANIZING FOR A SUCCESSFUL PRIVACY REGIME

We have already noted the difficulty when there is no Privacy Officer position, no stand-alone health information law, no designation of QGH as a "public body" and the consequential diminished accountability to the public for what is done with their personal health information. In addition, our audit revealed a somewhat confusing array of different 'privacy' policies and instruments not well understood by all staff in QGH. We could find no clear direction on the applicability of numerous privacy policies created by other GN bodies.

The GN website (www.gov.nu.ca) includes mention of the following documents:

> Acceptable Email & Internet Usage Policy (Department of Community and Government Services)
>
> Acceptable use of Mobile Devices Policy (Department of Community and Government Services)
>
> Records Management Policy (Department of Community and Government Services)

Social Media Policy (Department of Community and Government Services)

Archives Policy (Department of Culture and Heritage)

Video Surveillance and Recording in Schools Policy and Guidelines (Department of Education)

Access to Information and Protection of Privacy Policy (Department of Executive and Intergovernmental Affairs)

Privacy Breach and Incident Policy (Department of Executive and Intergovernmental Affairs)

The Government of Nunavut *Privacy Management Manual* (the Manual) is not listed as a Policy on the Government website. It is cross-referenced however in the Privacy Breach and Incident Policy which is listed on the website. The Manual and attachments is 132 pages. The eight sections are:

1. Privacy within the Government of Nunavut
2. Privacy and Communications
3. Creating Records in the Context of ATIPP
4. Privacy and Contracting
5. Privacy and Human Resources
6. Comprehensive Procedure for the Handling of Privacy Breaches and Incidents
7. Comprehensive Procedure for the Handling of Privacy Impact Assessments
8. Procedure for the Conduct of Privacy Inspections and Privacy Compliance Audits

There is a statement in the *Privacy Breach and Incident Policy* document on the GN Government website, that:

> "To support the Act [ATIPPA] and regulations, the PMM [Privacy Management Manual] will provide the tools needed to allow for the easy implementation of a standard privacy function that is consistent across all

> public bodies. For a detailed description of the measures and reforms required to respond to and prevent privacy incidents and breaches, please consult the PMM."

Our audit revealed very little familiarity with the Manual within QGH. Nonetheless, we considered each of these documents and the Manual to assess the value they might add to privacy compliance within the QGH. The first three sections of the Manual are impressive in terms of accurately reflecting the privacy expectations of any public body.

There are also sample forms and detailed procedures for the conduct of privacy inspections and privacy compliance audits. Despite the statement in section 8 of the Manual that the document is designed to "assist the ATIPP Manager and ATIPP Coordinators in their efforts to prevent privacy incidents and privacy breaches by identifying existing gaps and weaknesses in the systems, policies and practices of public bodies" we found no evidence that either privacy inspections or privacy compliance audits have been done in QGH prior to this audit.

There are problematic features of Section 6: Comprehensive Procedure for the Handling of Privacy Breaches and Incidents.

A distinction is made on page 35 between privacy incidents and privacy breaches as follows:

> **Privacy incidents** can be quickly and easily corrected without any prejudice to the individual. They are usually resolved immediately by the employees who become aware of them.
>
> **Privacy breaches**, on the other hand, may bring serious consequences for the individual and/or the GN, and they may require bold and comprehensive measures to minimize the damages. Consequently, they are the subject of systematic reporting and detailed response procedures.

There are several problems with this distinction. One problem is that the definition of a privacy breach in section 49.8 of ATIPPA makes no such distinction. It provides as follows:

> 48.8. For the purposes of this Division, a breach of privacy occurs with respect to personal information if

(a) the information is accessed and the access is not authorized under this Act;

(b) the information is disclosed and the disclosure is not authorized under this Act; or

(c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act.

Furthermore, the consequences of any given breach may not be immediately apparent. Particularly since the repercussions of any particular breach may be different for every affected individual. This view of something that can be called a "privacy incident" may motivate some employees to minimize a breach and not adequately consider the full impact and implications of a given breach. Tracking all breaches, whether major or minor, allows an organization to identify problem areas or problem practices and implement mitigation measures.

A much better approach is outlined in the 2013 *Guidelines for the Protection of Health Information* from the Canadian Health Informatics Association or COACH. This document defines a privacy incident as "a suspected single or series of unwanted or unexpected unauthorized use or disclosure of personal or personal health information". A privacy breach is defined as "a confirmed unauthorized or illegal use or disclosure of personal or personal health information."(p. 200)

The COACH distinction is more closely aligned with the requirements of ATIPPA than what is contemplated by the GN Privacy Management Manual.

Recommendation:

That for purposes of dealing with privacy breaches in QGH, all breaches be tracked and privacy incidents to be defined to mean only apparent breaches that haven't yet been confirmed.

RAISING THE BAR ON PRIVACY PROTECTION

Our Privacy Audit revealed that QGH does not have a recognizable privacy management program. We found that there is no comprehensive privacy training program for new hires nor in-service training on privacy best practices.

In Canada we now have more than 30 years of experience with privacy laws. Every jurisdiction in Canada has a public sector privacy law that defines "personal information" and then specifies the rules for the collection, use and disclosure of that personal information. In recent years there has been increasing attention to the need for public bodies to carefully organize themselves to enhance their transparency to the public and to bolster the level of privacy protection in all of their mandated activities. A good example of this is the revision of the OECD *Guidelines for the Protection of Personal Information* (the Guidelines) to focus on organization and leadership in public sector organizations. The Nunavut ATIPPA is essentially a first generation law modelled to great extent on the Ontario *Freedom of Information and Protection of Privacy Act* of 1988 which in turn is based on the Report of the Royal Commission on Freedom of Information and Individual Privacy of 1980- *Public Government for Private People*. Since the early days of privacy protection, the standards and expectations have been gradually strengthened.

PRIVACY MANAGEMENT PROGRAM

Those 1980 OECD Guidelines were reviewed and updated in 2013 in light of "changing technologies, markets and user behaviour and the growing importance of digital identities." The review of the guidelines, led in part by the former Privacy Commissioner of Canada, Jennifer Stoddart, determined that the original guidelines of 1980 remained sound and relevant. They were augmented in several respects however to address privacy management programmes, security breach notification, national privacy strategies, and global interoperability.

In 2013 the OECD revised guidelines[1] were issued –

The new **Part Three, Implement Accountability** provides:

15. A data controller should:

    a) Have in place a privacy management programme that:

        i. gives effect to these Guidelines for all personal data under its control;

[1] http://www.oecd.org/sti/ieconomy/privacy.htm

ii. is tailored to the structure, scale, volume and sensitivity of its operations;

iii. provides for appropriate safeguards based on privacy risk assessment;

iv. is integrated into its governance structure and establishes internal oversight mechanisms;

v. includes plans for responding to inquiries and incidents;

vi. is updated in light of ongoing monitoring and periodic assessment;

b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

This greater focus on a privacy management program is evidenced by the tool created by the Privacy Commissioner of Canada and her colleagues in British Columbia and Alberta - See also *Getting Accountability right with a Privacy Management Program*.

The foregoing statements relate to privacy protection in general. For health information specific advice, the QGH is encouraged to refer to the 2013 COACH Guidelines,

> Organizational culture comprises the assumptions, values, norms and behaviours of organization members. The protection of PHI in any organization depends on creating and maintaining a privacy-aware and security-conscious culture….Responsibilities need to be clearly assigned throughout the EHR governance and operational structure. [p. 54]

A well-planned privacy and security architecture framework can significantly contribute to an organization's effort to meet it privacy obligations and to put in place administrative, technical and physical safeguards, practices and procedures that:

> Protect the privacy of individuals' personal health information (PHI) in the course of providing services.
>
> Protect the privacy of individuals' personal information in the course of conducting corporate activities.
>
> Support compliance with the privacy legislation that affects the process of collecting, using, disclosing ,disposing or recording access to, use of or disclosure of PHI
>
> … [p. 287]

Recommendation

That the QGH develop a privacy management program to capture the role of a Privacy Officer, clear and accessible policies and procedures for the collection, use and disclosure of personal health information, staff privacy orientation and training and then, transparency of this program to the public. A relevant and useful guide is provided by the 2013 COACH Guidelines for the Protection of Health Information. Such a privacy management program might incorporate the relevant and appropriate provisions of the GN Privacy Management Manual that have been reviewed above, subject to the concerns already identified.

UNINTENDED CONSEQUENCES

In the course of our tour of QGH facility we observed brochures intended for the public which described the position of Quality Improvement Coordinator. The brochure invited patients with questions or concerns about hospital services to contact the Coordinator so that they can investigate and attempt to resolve the concern.

We learned that the QGH Quality Improvement Coordinator position was created after the Government of Nunavut had created its new Office of Patient Relations to "proactively address patient issues, concerns and questions along their health care

journey". When this was announced in July of 2013 it was stated that the new Office of Patient Relations:

- Provides information on the concern process;
- Assists patients and families in navigating the health care system;
- Directs patients and their families to the appropriate person within the system;
- Helps those with questions related to the rights of the patient, or concerns about care and services;
- Provides advice on conflict resolution for patients, families and hospital personnel;
- Investigates patient concerns and provides conclusions in a timely manner; and
- Makes recommendations to improve patient care following the investigation of a concern.

It appears that no consideration was given to how either the Quality Improvement Coordinator or the Office of Patient Relations will deal with privacy/access issues or complaints.

We recognize that there has been a welcome move across Canada to improve patient engagement in the health care context. This has been promoted by health quality councils and health ministries. [*A Resource Toolkit for Engaging Patient and Families at the Planning Table* (Alberta Health Services)]

This is manifest in tasking officials with promoting quality of care and ensuring involvement in decisions and respect for patients' preferences and empathy and emotional support for patients and families.

The experience in other Canadian jurisdictions however is that a significant number of the complaints that will be raised under this kind of quality of care regime will relate to either attempts to access the patient's own PHI or complaints about alleged privacy breaches. There is a potential for single-minded focus on the general patient complaints process to create confusion and conflicting approaches with the need to efficiently manage both privacy complaints and access by patients or their surrogates to their PHI. The right of access is straightforward and requires clear rules and processes to meet

the statutory requirements. The right of access is viewed by Canadian courts as a quasi-constitutional right of citizens.

In some Canadian jurisdictions with stand-alone health information laws guaranteeing the right of access, this right has been frustrated or even denied when there have been inefficient systems, lack of training, and lack of accountability. In some jurisdictions it is not well recognized that patients do not have to provide a reason why they seek access, the custodian cannot impose conditions on further use of the PHI and the concepts of data minimization and need to know have no application. Although inappropriate, the risk is that a request for access may be treated by a quality improvement coordinator or an Office of Patient Relations as a matter to be dealt with through discussion about motivation, and attempts to address that motivation or discontent instead of simply providing timely access to the PHI sought. It will be important to QGH to ensure that careful consideration is given to how to meet ATIPPA requirements and best practices and not to allow its quality of care processes to negatively impact ATIPPA requirements. This issue was considered in the Annual Report of the Saskatchewan Information and Privacy Commissioner 2007-2008 (p. 16):

> The position of QCC [Quality of Care Coordinator] was mandated for all Saskatchewan RHAs [regional health authorities] presumably in response to recommendations from the Fyke Commission and its focus on improving quality of care. I acknowledge that both of these positions need to be very much patient focussed. Nonetheless, there are significant differences in the two roles. For example, HIPA [Health Information Protection Act] sets out a simple and straightforward process for any individual patient or client to obtain access to their personal health information and, if there are errors, a simple process to seek amendment of the record. There are strict time lines and a right of appeal to our office if not satisfied with the RHAs response. There is a positive duty on trustees to assist the patient or client by responding to each access request openly, accurately and completely.
>
> We have in several formal reports discussed the importance of meeting access obligations and the limited opportunity for access to be denied. On the other hand, our experience is that a number of QCCs take a different approach in their dealings with patients/clients. This may involve protracted discussions or negotiations that include probing the motive and

intentions of the individual. This is not acceptable when dealing with access requests under HIPA or LA FOIP. It may involve taking additional time to consult with lawyers and risk management officials in the region to assess questions of liability and look to mitigate liability. Again, those issues are typically irrelevant in responding to HIPA access requests.

While both of these positions are important, as is the work they do in their respective regions, this work should not be done at the expense of statutorily mandated requirements such as HIPA. After all, HIPA is a statute, not just a policy directive. What's more, it is a special kind of law, on that the Supreme Court of Canada describes as "quasi-constitutional" and one that is normally paramount to other provisional laws. Yet, it appears that in some RHAs HIPA compliance has been designed to accommodate the quality of care initiative instead of the other way around.

Recommendation

That the Privacy Officer for the QGH work with the Office of Patient Relations and the Quality Improvement Coordinator to develop protocols to ensure that the information and privacy rights of patients are not in any compromised or diminished by the quality improvement initiative. This would include ensuring that through posters, brochures and the QGH, the public clearly understands the different roles of these offices.

STATUS OF NUNAVUT ELECTRONIC HEALTH RECORD

As noted earlier, all Canadian provinces plus the Yukon and NWT have agreed to build an electronic health record for every individual in their jurisdiction. This EHR would be interoperable so that PHI stored in one provincial EHR would, in appropriate circumstances become available to care providers treating that patient in another jurisdiction. Also, as noted earlier, this was the main motivation for the development of stand-alone health information laws in those other provinces and territories.

It appears that at one point the GN decided that it would also create an electronic health record. It appears that it developed a plan to do so. In the course of our audit we discovered a number of documents marked "DRAFT" related to that plan. These

appear to have been done with the assistance of outside consultants. Most of this work is dated in 2009 although we have discovered some documents dated as recently as 2011 and 2012. We understand that none of these documents are in currently in force in the QGH or anywhere else in Nunavut. These documents include:

1. EHealth Information Security Directive
2. Password Management for eHealth Systems Directive
3. Individual Access to Personal Information in eHealth Systems Directive
4. Monitoring and Audit of eHealth Systems Directive
5. Collection, Use and Disclosure of Personal Information in eHealth Systems Directive
6. eHealth Information Privacy Directive
7. eHealth Access Control Directive
8. Complaint Handling & Breach Management of Personal Information in eHealth Systems Directive
9. Retention and disposal of Electronic Personal Information Directive
10. Privacy Framework for Protecting Personal Information in the Government of Nunavut iEHR
11. iEHR conceptual PIA, Phase 2.1
12. Conceptual iEHR – Privacy and Security Architecture

A number of these documents are problematic. Almost none of the documents bear any resemblance to existing processes for PHI in the QGH.

This audit revealed that there is no iEHR at this time or even any components of the iEHR that exist in the form described in the above listed draft documents. There is however an electronic medical record deployed and currently used in QGH and throughout Nunavut. This is the Meditech system.

The Meditech system is clearly not an EHR as that instrument is defined by Canada Health Infoway. It is, rather, an electronic medical record -- typically something found in

physicians' clinics and smaller primary care centres. It will have an electronic record of health services provided by that clinic or primary care centre.

In contrast, the EHR envisaged by the Pan-Canadian Health Privacy and Confidentiality Framework and the Canada Health Infoway is comprehensive, includes PHI of all residents in a jurisdiction and is accessible by most healthcare providers and health care organizations. It would be comprised of domain repositories that are connected. There would be a domain repository for pharmaceutical prescriptions, another for laboratory test results and another for diagnostic imaging pictures and radiology reports. There would be a person or patient registry and another registry for health care providers. The iEHR would include PHI from hospital visits and visits to clinicians.

In addition there is Panorama, a public health and immunization domain. We learned that Nunavut may already be participating in Panorama.

It is very unclear whether the Meditech system can somehow be scaled up to become an iEHR as defined by Canada Health Infoway. Even if it can, it presently has almost none of the significant features of the iEHR. What exists in Nunavut is simply an electronic medical record for residents receiving treatment at QGH or one of the regional health centres. There is no significant correspondence between Meditech and the iEHR described in the draft documents.

It could be said that there is a glaring disconnect between the draft documents we reviewed and the actual systems and processes now in place at QGH. Examples of the gaps include the following:

- In none of the draft documents could we find any mention of the need for a new stand-alone health information law to permit the appropriate sharing of patient PHI in an EHR nor any mention of the inadequacy of ATIPPA for that purpose. There is no acknowledgement that virtually every other jurisdiction in Canada has opted to create a new stand-alone health information law to enable their iEHR. There is some suggestion that shortcomings in ATIPP could be adequately addressed by policy or procedures. This however flies in the face of the Canadian experience since 1997. Quasi-constitutional privacy rights of Canadians need to be transparent and accessible to patients and indeed all residents. Requiring Nunavut residents to review ATIPPA, which is not health specific and is a privacy law of general application, and then to search through

different GN policies to find out which parts of ATIPPA might apply and which would not is unreasonable.

- There is inconsistent use of "**Personal Information**" and "**Personal Health Information**". This is true of both the iEHR conceptual PIA and the Conceptual PIA – Privacy and Security Architecture. QGH is a large employer and will have a good deal of personal information of its employees, volunteers and perhaps contractors. This, however, is not required for the delivery of health care services which instead require personal health information. Comingling the two can create confusion and in turn compromise compliance with privacy requirements. A clear focus on personal health information which includes information about physical and mental health, about health services and about body tissues is essential in any health privacy regime.
- The draft documents largely ignore the office of the Information and Privacy Commissioner and its statutorily mandated role to oversee compliance with ATIPPA and privacy best practices.
- The various documents casually discuss implied consent as if it is already statutorily enabled. However, that is not the case and a reader of these draft documents would likely be misled into thinking that the implied consent, a feature of stand-alone health information laws in other jurisdictions, is also available to care providers in Nunavut. A careful reading of ATIPPA however reveals that consent, when it is required, must be written express consent. There is no provision for implied consent.
- Reference to a confidentiality undertaking required of all staff is unhelpful since it blends together the concepts of confidentiality and privacy. The undertaking required of health staff, including all QGH staff, must address privacy requirements and compliance with ATIPPA.

The Assistant Deputy Minister advises that she intends to arrange for a detailed review of the earlier documents relating to a future electronic health record as well as the nine directives and welcomes input from this office on revision of those documents. Apart from this Audit Report, I intend separately to provide QGH and the Department of Health with my detailed comments with respect to the directives to assist those officials in their review and revision of such documents.

If there should be any intention to wait on revision of these documents until a comprehensive electronic health record exists in Nunavut, that would be a mistake. What is required is a strong privacy culture within the QGH now. Although this also is important whenever an electronic health record is implemented, the need for privacy leadership, good training and appropriate policy and procedures is evident now. To achieve robust privacy protection will then simply facilitate a smoother implementation of the electronic health record at some future date.

Recommendation:

That the Department of Health proceed with its stated plan to consider implementing an electronic health record and ensure that the appropriate policies and procedures are in place to accommodate that.

HEALTH RECORDS

In any hospital, health records and the manner in which they are handled is one of the most important elements of a robust privacy regime. Given the importance of this unit to maintaining the control and integrity of vast amounts of personal health information, and given the daily responsibility to make decisions about patient access requests and requests for disclosure to third parties (both consented and non-consented), this unit could be seen as the foundation for the QGH privacy regime. In many Canadian hospitals, it is the health records office that is a leader in terms of promoting privacy compliance throughout the institution. The Health Records unit must be very knowledgeable about the relevant provisions of ATIPPA, and privacy best practices. In most jurisdictions, health records units will have some responsibility for training almost all hospital staff on privacy requirements and may expect to be a place of first resort when other staff have questions about patient access, use and disclosure of PHI. This becomes even more important when there is no designated and appropriately trained Privacy Officer at QGH.

In the 2013 COACH Guidelines, the description of Health Records is as follows:

> Health Records is responsible for protecting PHI contained in health records in paper and electronic form, which may include:
>
> - Responding to requests for the release of subject of care information;

- Authorizing the release of, and access to, PHI for research and other non-care-related purposes;
- Developing departmental policies and procedures to support the secure access, retention, destruction, storage, transfer and release of PHI;
- Ensuring office and storage areas are physically secure to prevent unauthorized access, loss or theft of PHI;
- Participating in regular educational awareness initiatives;
- Reporting known or suspected information security incidents promptly.

Our observation is that the QGH health records department could benefit from more rigour in protecting patient PHI. We learned that health records staff had available to them two binders with some policy and procedures they needed to be familiar with. We reviewed those binders but there was no detailed information about privacy and privacy best practices in a healthcare context. If that kind of information is not readily available in the health records department, one can imagine the difficulty a hospital employee might have trying to obtain answers or clarity on a time sensitive privacy issue. The binder contents were mostly focussed on various procedures for opening and managing paper patient files. We found stacks of patient files sitting on unattended desks. Senior staff we spoke to when we toured this unit had little familiarity with ATIPPA or privacy best practices. The records unit is not responsible for ATIPPA or privacy training for new hires in the hospital.

We could see no evidence of any effort to inform the public or patients of their information/privacy rights. There is no information about the obligations of the Department to provide patients with their information within the statutory time limit of 30 days. There is no information about the limits on what the QGH can do in terms of collecting, using or disclosing their PHI. There is no information about the ability of an aggrieved patient to make a complaint to the Information and Privacy Commissioner, an independent office of the Legislature with the mandate to investigate just such complaints. There were no posters, brochures or other literature explaining the patient's right to see their own personal health information and to seek to have errors corrected. Apparently access by patients to their own PHI is seen as a reactive process that must be initiated in every instance by the patient.

To complicate matters, the current QGH health records system is a hybrid system with some records in digital format in the Meditech system but many other records in hard copy format. That means an access request from a patient for their own PHI requires both a search of the Meditech records for that patient but also a search of hard copy records to ensure that all relevant information is identified. Such a hybrid records system increases the risk that not all relevant information will be identified when it needs to be and that more time and effort that would otherwise be necessary will be involved in both treatment activities and responding to access requests. This hybrid record system has continued for some time and we could not determine a hard deadline when all records will be migrated to the Meditech system, though there were some indications that part of the reason for the delay in this transition was the reluctance of physicians to use the system.

As noted in the 2013 COACH Guidelines for the Protection of Health Information,

> Hybrid records present unique privacy and security challenges to PHI, the evidentiary value of the records and continuity of care. A primary consideration is whether, and to what extent, paper or older records should be migrated into the electronic recordkeeping system or be archived. It is critically important to choose a method of migrating and archiving information that ensures confidentiality is upheld, information is available as needed and integrity is retained. In some jurisdictions a privacy impact assessment may also be required when making such a transition, and certainly a security assessment of both the process used to make the transition and the new system should be done." [p. 268]

With the conversion from paper to digital form, the Guidelines state:

> The process must involve some form of quality assurance of the transfer and the resulting output. This could include, for example, periodically comparing a randomly selected digital copy to the original. A record of the quality assurance steps taken and the outcomes should be maintained. Digital copies of records should be kept in a read-only format so that they cannot be altered after conversion, although some can be searchable. The image or digital version should be identical to the original paper version.

In addressing privacy education of all QGH employees, there are two relevant lessons from the experience in hospitals in other parts of Canada. The first is that the best education is focussed on what employees in any particular department need to know with respect to the types of services they provide and the kind of PHI they typically deal with. This is supported by case studies and checklists. The second lesson is that most privacy problems tend to arise in four areas: patient access to their own PHI; consent -- what it looks like and when it is needed; disclosure to third parties, particularly non-consented disclosure of PHI; and security -- in other words, the administrative, technical and physical measures necessary to reasonably protect the patient PHI. Any training should put a particular focus on addressing these four predictable problem areas.

Recommendation:

Ensure that all health records staff receive adequate training with respect to relevant requirements of ATIPPA as well as privacy best practices.

That the Health Records office and operations be reviewed to determine improvements that can be made to security of the paper files, ensuring a sign out/ sign in procedure to ensure tracking of movement of the patient file within QGH.

Implementation of a clean desk policy to prevent the accumulation of patient files on unattended desks in the Records Department area.

Limit the opportunity for other hospital staff to access patient paper files without a clinical purpose.

Consider how the Health Records office can provide more support to QGH staff in adopting and following ATIPPA compliant procedures and privacy best practices as outlined in the 2013 Guidelines of COACH.

That QGH develop a comprehensive plan including a deadline to complete the conversion of paper records to digital format including undertaking a security assessment of the process and the Meditech system.

That the QGH consider developing a Privacy Charter modelled on the sample in Appendix B to the 2003 COACH Guidelines. This would be based on the QGH's

privacy and information handling policies and would be available to patients and the public.

That QGH develop and disseminate informational brochures, posters and other educational materials for the general public outlining their rights with respect to access to their own personal health information and with respect to appropriate collection, use and disclosure of their PHI and how they can address concerns about these things.

SECURITY

s. 42 of ATIPPA requires that:

> 42. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This also applies to QGH even though it is not a separate public body for purposes of ATIPPA.

I encourage QGH to review a very helpful discussion of security safeguards in the 2003 COACH Guidelines at pp 147-224.

In most Canadian stand-alone health information laws those reasonable arrangements must address physical safeguards, technical safeguards and administrative safeguards. Physical safeguards involve such things locked doors, clean desks and locked file cabinets. Technical safeguards involve encryption, privacy screen notices, and timing out features on computers. In terms of technical safeguards compliance would require following the ISO/IEC 27002 and as well the security safeguards discussed in the 2003 COACH Guidelines, pp 147-223. Administrative safeguards involve policies, procedures, the creation of a Privacy Officer position within an organization and having good privacy materials available for staff and the public.

Safeguards against breaches of privacy might be categorized as soft or hard. ‘Soft' safeguards are things like requiring employees to provide a privacy pledge or oath, providing robust training, providing staff with a comprehensive set of policies and procedures for privacy protection. When the soft safeguards fail to deter improper collection, use or disclosure of patient PHI, there are a number of possible ‘hard'

safeguards. These would include disciplinary action including dismissal, a prosecution under a stand-alone health information law or in some cases under the Criminal Code, administrative penalties imposed by a health profession regulatory body and class-action lawsuits seeking damages for breach of privacy.

The Canadian experience with stand-alone health information laws and electronic medical records/electronic health records is that the biggest risk is usually improper use or disclosure of PHI by healthcare workers. Consequently QGH should ensure that it has in place the appropriate soft safeguards.

Certainly one of the most common soft safeguards is requiring staff to pledge to protect the privacy of patients and the confidentiality of patient PHI. In the course of our QGH audit, we were frequently directed to the ‘Confidentiality Oath' required to be taken by all new QGH/GN employees. This states as follows:

OATH TO BE TAKEN BY EMPLOYEES OF GOVERNMENT OF NUNAVUT

OATH OF OFFICE AND SECRECY

I,_____, solemnly affirm and declare that I will faithfully and honestly fulfil the duties that devolve upon me by reason of employment in the Public Service of the Territory of Nunavut and that I will not, without due authority, disclose or make known any matter that comes to my knowledge by reason of such employment.

_____

Signature of Employee

Subscribed before me this _____ day of _____A.D./_____

_____

Commissioner of Oaths for the Territory Of Nunavut

My commission expires _____

This form is problematic for the following reasons:

1. Such an oath is so wide that it captures anything learned by any GN employee and by indiscriminately applying to "any matter that comes to my knowledge by reason of such employment", there is no appropriate focus on personal health information of patients. It treats any written process for scheduling staff vacations, staff payment procedures or how to change toner in the photocopy

machine no differently than the PHI of a patient. Aside from the fact that employees will learn all kinds of things in the course of their employment that will be either public record or appropriately available to citizens or are matters of little consequence, indiscriminate lumping of all such information in with PHI completely fails to put employees on notice that they must comply with privacy policies of the QGH.

2. There is no reference to either personal information or the ATIPPA. The obligation of staff and their public body employer is to comply with all requirements of ATIPPA which includes how personal information is collected, used and disclosed. It also includes how access can be obtained and how incorrect information can be challenged. The oath however fails to bring home to any employee that they are bound to comply with ATIPPA and all of its requirements.

3. The phrase "disclose or make known" ignores the obligations of any employee to comply with the rules for collection and use of personal information. Disclosure is but one of the processes limited by the provisions of ATIPPA.

4. The focus on disclosure reinforces old notions of confidentiality but completely fails to alert the employee to the privacy regime created by ATIPPA. Confidentiality is different than privacy. The definitions that need to be clear to all employees would include these:

    (a) Privacy means the right of the individual to exercise a measure of control over their own personal information or personal health information. It includes the ability to refuse to share certain information, the right to obtain access to information held by public bodies about them and strict limits on how that information can be collected, used and disclosed and the ability to complain to an independent privacy oversight body i.e. the Information and Privacy Commissioner.

    (b) Confidentiality means the protection of the personal information or personal health information from those who have no legitimate need to know that information. Every confidentiality breach is a privacy breach but every privacy breach doesn't involve a confidentiality breach.

    (c) Security is a means by which confidentiality is achieved and is the means by which personal information or personal health information is protected

from those inside or outside of the public body who have no legitimate reason to view or access that information.

5. A more general concern is that such an Oath completely fails to acknowledge the obligations for any public body to operate transparently, a quasi-constitutional requirement, equal in importance to the obligation to protect information privacy of citizens. This focus on "secrecy" operates to undermine the access to information obligations under Part I of ATIPPA.

6. Any oath or affirmation is of little value unless it is supplemented and supported by a robust privacy training program for all new hires, reinforced by regular in-service privacy training of all staff and enabled by comprehensive, high quality training materials including checklists and sample forms. The oath can be a useful supplement to a robust training program but is certainly no substitute for such training.

We reviewed the QGH Administrative Policy – Confidentiality. This was last revised on 22/11/2015. This presumably was intended to be something of an overarching policy statement on privacy expectations for employees of QGH.

Its focus is less clear when one considers the opening statement that: "Information pertaining to patients, staff and hospital operational/management issues shall be respected, communicated and maintained in a manner that safeguards privacy." Instead of being a clear statement about protecting patient PHI, it is conflated with hospital operational issues that may have nothing to do with PHI. Item #4 also includes information about facility operations in the requirement that staff shall not access or disclose such information. In addition to mixing different kinds of information, the requirement does not address the improper use of PHI but only deals with access or disclosure. Item #5 addresses not PHI but rather personal employee information.

Item #6 requires immediate supervisors to "educate all new employees on methods of safeguarding information and necessary authorizations for the collection, use and disclosure of personal or health information." The 2013 COACH Guidelines describe the education and awareness programs as follows, in part:

> Regardless of the goals, the most effective education and awareness programs employ a variety of strategies to support different roles and responsibilities and different learning styles. These strategies could

include classroom training, online training, training by superiors and hardcopy materials.

All employees should be required to attend regular privacy/security awareness sessions, which should always be included in employee orientation. Job transfers and reassignments provide excellent opportunities for employees to review security policies and procedures.

Education programs should:

- Clarify appropriate behaviour for handling information;
- Explain penalties (corrective controls) for breaches of security or privacy;
- Include role-specific training for administrators.

Healthcare organizations should document, track and monitor an established performance indicator for known or suspected privacy breaches and security incidents and assign responsibility for addressing both threats and incidents. Breach and incident reports should be shared with a user's manager or supervisor, Human Resources, IT and the privacy officer to document, follow up and prevent similar breaches and incidents from recurring. [p.83]

Our audit found that this was either not being done or at least not done in a way that provided employees with a comfortable understanding of what can be done and must not be done with patient PHI. The three principles itemized on page 2 are weak in that they appear to blend confidentiality and privacy without any explanation in the policy that there is a difference. The definition of ‘confidentiality’ as "the obligation of a person or organization to preserve privacy" is inaccurate and again would not help the reader have any better understanding that confidentiality is but one element of privacy and that privacy is focused on the patient and the patient's wishes and expectations whereas confidentiality is focused just on the PHI itself.

We saw no particular protocols or policies addressing interpreters working in QGH. An additional challenge for QGH is the requirement to be able to deliver services in French and English, Inuktitut and Inuinnaqtun. We understand it can be difficult to hire interpreters who also have clinical experience. That suggests that a particular focus on privacy training must be to ensure that interpreters have a comfortable understanding of privacy and privacy requirements for QGH.

In sum, this skeletal document (two pages) attempts to cover too much ground and fails to inform any employee, physician, volunteer, student, researcher or contractor of the full dimensions of privacy and privacy obligations.

MEDITECH INFORMATION SYSTEM

We learned that this system was implemented in QGH in 2011. By 2017 it is intended that this Meditech system will be in every Nunavut community. This is an electronic medical record but not an electronic health record as that term is defined by Canada Health Infoway. It is not populated with PHI of all Nunavut residents to include prescription drug information, laboratory test results and diagnostic imaging pictures and reports. It is a system to capture information collected by QGH in the course of treating those individuals.

There are three systems coordinators who do the training for QGH staff and provide 24 hour support to health facilities in five other communities in Nunavut. The IT unit also includes two individuals responsible for maintaining the computer hardware and a systems analyst who does custom report writing. There is a person dealing with digital imaging and a clinical information specialist. We learned that one identified problem is a high rate of turnover in this unit and that there are currently vacancies for clinical specialists, training and development officers. It apparently takes one or two years to fill a position. Part of the challenge is finding individuals with a clinical background as well as the technical expertise.

We further learned that the only privacy training would be ‘on the job' training from colleagues in their particular units not from the IT staff. Training by IT staff is focused on technical features of Meditech and how to input and access data. This general training is provided before any new hire is allowed access to the Meditech system.

We were advised that the particular Meditech application in QGH does not have any kind of proactive audit program. It does have a reactive audit capability which is complaint driven. If a complaint is lodged, QGH can have IT staff perform an audit and can track who accessed what part of the chart in question, what pages they looked at, and when they did it. The experience in other jurisdictions with longer experience with electronic health records is that it is important to be able to do proactive audits and to ensure that all hospital staff are aware of those proactive audits to discourage snooping. Furthermore there is no particular protocol involving both the IT team and the

human resources office so that once an employee leaves the employ of QGH their access to the system is terminated immediately. We were told that if a user hasn't used the Meditech system in 4 to 6 months, their accreditation will be revoked. Such a relaxed approach is unacceptable.

Apparently there originally was a field for ‘reason to visit' that users had to complete. That was apparently removed after some complaints from users that completing this field of information was inconvenient.

For Meditech there is no masking functionality which would allow all or certain elements of a patient's PHI to be rendered unavailable to a user of the system without express consent of the patient.

All access to the Meditech data is "role-based". This means however that any health care worker can be accredited as a user so long as they are employed by QGH or the Department of Health and are engaged in diagnosis, treatment or care of patients. There is no provision for testing the privacy literacy of any employee before they are accredited as a user. There is nothing to stop an employee who has little or no understanding of privacy and privacy best practices from becoming an accredited user and thereby afforded access to all patient data in the system used by the QGH.

We learned that QGH staff have been known to search their own PHI through Meditech, a practice that would be inconsistent with privacy rules and best practice. There are undoubtedly incidents of employees looking up the records of friends and relatives. There is, however, no way to pro-actively monitor these unauthorized accesses so as to deter such activity.

During our interview with the IT unit, we learned that several committees were created by the Department of Health to deal with privacy and privacy directives at about the time the Meditech system was implemented. These privacy directives will be discussed in another section of this report but our understanding is that none of these have been implemented. Certainly most of the other interviewees in QGH were not familiar with those privacy directives.

Recommendations:

There should be comprehensive compulsory privacy training with appropriate privacy training materials for all QGH staff. This should include training on the Meditech system.

No employee should become an accredited user of Meditech unless there is evidence they have successfully completed the privacy training.

When any employee attempts to enter the Meditech system, the screen should display a caution against any collection, use or disclosure without a legitimate need for that employee to know the subject PHI.

The 'reason to visit' should be a required field for any employee entering the Meditech system.

QGH should develop a masking option which would allow a patient to designate certain elements of their PHI not to be accessible without the patient's express consent.

The QGH should ensure that access to Meditech is closed immediately upon any employee no longer requires access whether by resignation, dismissal or change in position or for any other reason.

There should be a policy/procedure for suspending Meditech access privileges for anyone who has abused their user privileges.

The system should be configured so that it can randomly and pro-actively monitor access to the system and raise flags where anomalies are detected so that unauthorized access can be minimized.

FAXING

We found in the audit that there is a good deal of "faxing" still used to transmit or receive PHI of QGH patients to or from other health centres or a variety of third parties. We determined in our audit that there is no written policy or procedure to guide staff using fax facilities. We also learned that misdirected faxes have occurred, and that faxes are often left in places where the content is readily available to a number of others who have no reason to know the content about certain patients. A resource we would recommend to QGH is the tool developed by the Saskatchewan Information and Privacy Commissioner Office - *Faxing Personal Information and Personal Health Information – Safeguards and responding to a breach* at

http://www.oipc.sk.ca/Resources/2014-2015/Faxing%20PI%20and%20PHI%20-%20Safeguards%20and%20Responding%20to%20a%20Breach.pdf

Recommendation:

That QGH develop a comprehensive policy for fax transmissions and the process when there are misdirected faxes.

That QGH ensure that fax machines are in secure areas of the facility not accessible to the general public.

EMAIL /TEXTING

We reviewed several documents that appear to overlap to some extent. This includes:

> QGH Clinical Procedure – E-mail consultation, (Revised: 04/094/2008)
>
> Acceptable Email & Internet Usage Policy (Department of Community and Government Services (CGS) (Revised Oct. 5, 2005)
>
> Health Directive – Sending a Receiving Confidential Email and Mail, A-01, Feb 22, 2016 ("Applies to All Health")

The QGH Clinical Procedure document is sparse and provides little helpful practical advice beyond incorporating by reference the Archives Act, ATIPPA and the Government of Nunavut Acceptable Email Use Policy.

The Community and Government Services document is very broad in scope and is not in any way focussed on privacy or the protection of personal health information.

The Health Directive has some appropriate and important information for healthcare workers. We identified some concerns however with the document.

The Health Directive starts with the problematic sentence: "The Department of Health (Health) must provide a process of due diligence in order to ensure **the circle of care** protects its clients, staff, department and the overall Government of Nunavut." [emphasis added] This statement uses a term - circle of care - that is not found in ATIPPA and in fact that has proven confusing in the context of electronic health records. The proper approach is to assess whether a health care provider has a legitimate 'need-to-know' a person's personal health information - not whether they may

feel they are somehow in something called a circle of care. In any event, even if one uses the ‘circle of care' concept, it may be different for every patient and indeed for every patient's individual episodes of care. Just because you may have treated a patient at some point for one ailment does not mean you are entitled to view all of that person's PHI just because you work in the same facility as those who are providing diagnosis, treatment or care for the same person but for a different presenting health problem.

The discussion of verbal consent ignores the reality that ATIPPA does not permit verbal consent. Consent when required must be in writing.

Furthermore, it conflates personal information of employees and confidential but not personal information and neither single out personal health information as being different from personal information. Confidential means not just personal information but also "business information, business sensitive" or " staff information for staff records." The focus on confidentiality rather than privacy may be confusing for staff who have not had clear direction on the difference between the two.

It is important to ensure that emails and text messages are made subject to the same record retention and destruction schedules that apply to paper records.

Recommendations:

That QGH develop an appropriate email/texting policy that specifically addresses personal information and personal health information.

MOBILE DEVICES

We learned that many QGH staff including physicians bring their mobile device to work and may use their mobile device to record at least some PHI. The QGH doesn't have its own mobile device policy. There is however an instrument described as the *Community and Government Services Acceptable Use of Mobile Devices Policy* we obtained from QGH. This policy is stated to apply "to all GN employees, contracted resources and any additional users that use mobile devices to access, store, back up or relocate any Government of Nunavut or client-specific data." The policy appears focussed principally on connectivity of all mobile devices on the core GN network. There is no mention of Meditech presumably since this is not a policy that originated in the Department of Health. The result however is that there is very little useful direction to physicians or

QGH employees who bring their own mobile device to work and may use this with or without connecting to the "core GN network". That leaves open to abuse, health care workers taking screen shots of Meditech data or uploading PHI of QGH patients in their own mobile devices. Nor is there any clear policy on encryption or password protection of mobile devices such as phones, tablets, jump drives and other portable storage devices.

Recommendation:

That QGH develop a mobile device policy for its employees, contractors and students that addresses both connecting with the Meditech system as well as the use of mobile devices brought into QGH by those individuals and utilized to collect PHI of patients. The 2003 COACH Guidelines provide an excellent set of security controls for mobile devices [p. 290]

SOCIAL MEDIA POLICY

QGH does not apparently have a social media policy but such a policy has been developed by Executive and Governmental Affairs. The policy appropriately recognizes the need to address ATIPPA provisions in determining what information may be released on social media. Implementation of this policy would likely be enhanced by the existence of a QGH Privacy Officer who would be able to ensure that any social media posts would be consistent with the ATIPPA. On page 6 of the instrument there is a specific section entitled Access to Information and Protection of Privacy. This section is quite comprehensive in its consideration of ATIPPA and risk mitigation.

OUTSOURCING ARRANGEMENTS

I reviewed the current Health and Medical Services Agreement between the GN and the Ottawa Health Services Network Inc. (OHSNI) dated April 2011. This creates an arrangement where certain specialist health and medical services can be provided by Ottawa health facilities to persons residing in Nunavut. Fourteen such health services are particularized in the document. The agreement provides for the transmittal of medical records and patient discharge reports between OHSNI and the Nunavut Department of Health. This includes an agreement that the Department of Health "shall ensure that all Health and Medical Records are accurate and available in a timely

manner to OHSNI Personnel treating a Patient." Also included is a provision that "patient medical information is confidential and that OHSNI must use its discretion in disclosing information. Consequently, OHSNI will not be held liable for the release of personal medical or health information, which, in the reasonable discretion of OHSNI was necessary or appropriate under the circumstances." [p. 9]

There is a section entitled Confidential Information. It provides as follows:

> The DHSS and OHSNI agree that either Party may identify information arising out of this Agreement as being confidential and upon notification to the other Party such information will be treated as confidential by the notified Party. For greater certainty:
>
> (a) OHSNI shall ensure that confidential Information obtained from or concerning GN and DHSS shall be kept confidential and used only for purposes required for the performance of the Services and that all OHSNI Personnel, employees, agents, or sub-contractors who perform or assist in any way, direct or indirect, with the performance of the Services shall have first assumed with OHSNI obligations of confidentiality at least equivalent to those assumed by OHSNI hereunder.
>
> (b) OSHNI shall not allow or participate in any media coverage or statements regarding the Services or related information, except with the prior written consent of the Minister, and in accordance with the requirements of the [ATIPPA], the Financial Administration Act, and all other applicable GN laws and policies.

We have not been able to determine whether the Department of Health has identified and designated that all PHI in its custody or control and shared with its external contractor is "confidential information". That would be necessary to ensure that the PHI of Nunavut residents, once made available to OHSNI, would continue to be protected.

We also examined the written agreement between the GN and the Ottawa Hospital whereby the Hospital supplies pharmacy consulting advice and services dated in April 2016.

Clause 11.4 provides as follows:

11.4 Any information obtained from, or concerning any department of the GN, or clients of any department of the GN, by the consultant, its agents or employees in the performance of the Services, or of any other contract, shall be confidential. The consultant shall take such steps as are necessary to ensure that any such information is not disclosed to any other person, and shall maintain confidential and secure all material and information that is the property of the GN and in the possession or under the control of the Consultant. This clause survives termination or expiry of this Agreement.

The failure to acknowledge the sensitivity of personal health information and the statutory duty to protect that personal information is a deficiency. To treat any and all information concerning any department of the GN or information obtained from that source the same way as personal health information is likely to diminish the attention that personal health information warrants. Therefore, the general confidentiality clause noted above is inadequate.

Recommendation:

That QGH ensure that any contracts that involve personal health information of patients of the QGH specifically identity what can and cannot be done with that PHI. All such contracts should explicitly incorporate by reference the privacy requirements imposed on any public body by ATIPPA.

DISCLOSURE OF PHI TO THIRD PARTIES

In our audit we heard concerns about how and when patient PHI can be disclosed without consent to third parties. This might be a request from police, an insurance company or perhaps an office of the legislature (other than the Information and Privacy Commissioner). ATIPPA certainly allows disclosure of personal information to third parties with the written consent of the patient. If there is no consent, then we suggest the following checklist:

- Has the third party provided authority in writing of one of the 22 subsections of s. 48 of ATIPPA that might permit disclosure?
- Is there authority in one of the 22 subsections of s. 48 of ATIPPA?

- Is the request for disclosure properly documented so that the QGH has a record of the request?
- Is the purpose of the disclosure clear?
- Have steps been taken to ensure that the least amount of personal information which is necessary for that purpose is disclosed?
- Has QGH retained a record of the disclosure and relevant documentation?

In terms of disclosure of personal information to police, many hospitals across Canada have found it useful to arrange for protocols with local police forces to minimize conflict or confusion when police request personal information of patients at those hospitals. In this regard, we note that the Memo dated March 17, 2014 *Disclosure of Personal Information to Law Enforcement and the Fact sheet: When the RCMP come to call* were presumably developed to assist both police and QGH employees with disclosure of PHI.

Recommendation:

That the QGH consider a checklist for non-consented disclosures of PHI to third parties:

- **Has the third party provided authority in writing of one of the 22 subsections of s. 48 of ATIPPA that might permit disclosure?**
- **Is there authority in one of the 22 subsections of s. 48 of ATIPPA?**
- **Is the request for disclosure properly documented so that the QGH has a record of the request?**
- **Is the purpose of the disclosure clear?**
- **Have steps been taken to ensure that the least amount of personal information which is necessary for that purpose is disclosed?**
- **Has QGH retained a record of the disclosure and relevant documentation?**

That all staff working in Health Records, the clinics, OR and Emergency be made familiar with the two documents (Memo dated March 17, 2014 *Disclosure of Personal Information to Law Enforcement and the Fact sheet: When the RCMP come to call*).

IS THERE A CULTURE OF PRIVACY IN QGH?

We did not, of course, canvass all current staff in QGH. Our observations, findings and recommendations are however based on interviews with department heads, the materials we reviewed, the absence of comprehensive written policies, procedures and training materials and the lack of a clearly identified privacy leader in the organization. We certainly encountered individuals who have had considerable experience in hospitals and health regions with more developed privacy regimes. We also could see evidence of heightened privacy awareness among certain of the health professionals we encountered. As noted elsewhere, we also encountered a widespread belief that a lot more could be done in QGH to promote privacy and privacy best practices. All of this leads us to believe that if the recommendations flowing from this audit are implemented, QGH staff have an appetite for such change.

Notwithstanding those positive impressions, we could find little evidence of an existing culture of privacy and general adherence to privacy best practices. The absence of a Privacy Officer, properly mandated and resourced, lack of written policy and procedures, absence of a rigorous training program for new hires and for in-service training and weaknesses in the existing electronic medical record system (Meditech), and weakness in out-sourcing contracts all indicate serious deficiencies in the QGH culture.

There are no privacy screens on a number of computers, too many duplicate copies of documents replete with PHI of patients, and missing denial of access to Meditech users who do not use the system for a period of time. We also learned that staff have been observed using the Meditech system to read their own PHI recorded in the system. This kind of abuse of the Meditech system for illegitimate purposes is troubling. It is indicative of a casual approach to privacy that needs to be changed. Although there are some policies and procedures available to clinical staff and other policies on the Y drive, we heard these are not universally accessible and are not well organized. In addition some policies are only in the GN network that all staff may not have access to. We heard of a Policy, Planning and Procedures Committee chaired by the Department of Health Director of Policy but any products produced by that committee are not widely available to all hospital staff and are not even widely understood.

We learned that there is still frequent use of fax machines and fax technology, particularly in communication to or from QGH and community health centres throughout Nunavut. We learned of an auto-print feature of some electronic equipment in QGH

which typically results in numerous copies of PHI left lying in plain view of persons who have no legitimate need to know that PHI. There have certainly been misdirected faxes in the experience of clinical staff but apparently no particular policy that covers faxing procedures and how to respond to misdirected fax messages.

We had the opportunity to meet with a clinical nurse educator and former manager of inpatient care. She provides orientation to new nursing staff. This is apparently open to any employees but is not mandatory. Apparently managers in the different departments are supposed to be doing their own privacy training but we frankly saw little evidence of this.

We learned that nursing students from Nunavut Arctic College routinely come into QGH to work as part of their training program. They are accredited for use of Meditech but there is no satisfactory process to terminate their access privileges when they complete their term in QGH.

Our conclusion therefore is that considerable work needs to be done to promote a strong culture of privacy in QGH. Our hope is that this Audit Report will be helpful to QGH in focusing its efforts to bolster privacy protection.

SUMMARY OF RECOMMENDATIONS

1. That the QGH and all other health facilities in Nunavut be designated in the ATIPPA Regulation as a "public body".

2. I recommend that the GN develop a stand-alone health information law similar to such laws in other Canadian jurisdictions. This would include a broad definition of personal health information, a clear definition of who would qualify as a custodian and appropriate rules for the collection, use and disclosure of personal health information. This should also include a statutory right of anyone to request access to their personal health information and the right to request that errors be corrected. The custodian should be subject to an explicit duty to assist applicants in exercising their right of access. The approach to consent should be one focused on implied consent to align with the approach in other provinces. This would be subject to certain kinds of disclosure requiring express consent and for a limited number of purposes no consent required. I recommend that the Information and Privacy Commissioner be the oversight office to ensure that there is some consistency in the approach to privacy compliance overall in Nunavut.

3. My recommendation is that the focus should be on ensuring that the law is as straight-forward and accessible as possible. That should facilitate better understanding and ultimately higher levels of compliance at QGH.

4. I recommend that QGH appoint a Privacy Officer with the following features:

    - Designated leadership role to lead the privacy compliance efforts in QGH;
    - Sufficiently senior to be able to have ready access to the CEO and senior management;
    - Mandated to develop a comprehensive privacy management program;
    - To provide input to the CEO and senior management on achieving good privacy compliance in new programs, new software and policies;
    - To be responsible for developing a full suite of written policies and procedures for privacy compliance and to oversee staff privacy training both the orientation of new hires and in-service training for existing

employees as well as volunteers and contractors;

- To ensure proper privacy protection in out-sourcing contracts that involve significant volumes of personal health information;
- To be the key liaison between the QGH and the Office of the Information and Privacy Commissioner;
- To be closely associated with the Records Department and the IT department to ensure that privacy considerations are regularly and fully canvassed by those departments in the course of their work;
- To consider how to ensure that information about patient's privacy rights are brought to the attention of patients and the public by means of brochures, posters and the QGH website.
- To take steps to ensure that the QGH Quality Assurance Coordinator and that officer's work do not in any way interfere, obstruct or impair the role and focus on the Privacy Officer and the privacy rights of patients and members of the public. This would include at a minimum ensuring that the Coordinator receives appropriate privacy training and that there is clear communication between the Coordinator and the Privacy Officer.

5. That for purposes of dealing with privacy breaches in QGH, all breaches be tracked and privacy incidents to be understood to mean only apparent breaches that haven't yet been confirmed

6. That the QGH develop a privacy management program to capture the role of a Privacy Officer, clear and accessible policies and procedures for the collection, use and disclosure of personal health information, staff privacy orientation and training and then, transparency of this program to the public. A relevant and useful guide is provided by the 2013 COACH Guidelines for the Protection of Health Information. Such a privacy management program might incorporate the relevant and appropriate provisions of the GN Privacy Management Manual that we have reviewed, subject to our concerns already identified.

7. That the Privacy Officer for the QGH work with the Office of Patient Relations and the Quality Improvement Coordinator to develop protocols to ensure that the information privacy rights of patients are not in any compromised or diminished by the quality improvement initiative. This would include ensuring that through

posters, brochures and the QGH, the public clearly understands the different roles of these offices.

8. That the Department of Health proceed with its stated plan to consider implementing an electronic health record and ensure that the appropriate policies and procedures are in place to accommodate that.

9. Ensure that all health records staff receive adequate training with respect to relevant requirements of ATIPPA as well as privacy best practices.

10. That the Health Records office and operations be reviewed to determine improvements that can be made to security of the paper files, ensuring a sign out –sign in procedure to ensure tracking of movement of the patient file within QGH.

11. Implementation of a clean desk policy to prevent the accumulation of patient files on unattended desks in the Records Department area.

12. Limit the opportunity for other hospital staff to access patient paper files without a clinical purpose.

13. Consider how the Health Records office can provide more support to QGH staff in adopting and following ATIPPA compliant procedures and privacy best practices as outlined in the 2013 Guidelines of COACH.

14. That QGH develop a comprehensive plan including a deadline to complete the conversion of paper records to digital format including undertaking a security assessment of the process and the Meditech system.

15. That the QGH consider developing a Privacy Charter modelled on the sample in Appendix B to the 2003 COACH Guidelines. This would be based on the QGH's privacy and information handling policies and would be available to patients and the public.

16. That QGH develop and disseminate informational brochures, posters and other educational materials for the general public outlining their rights with respect to access to their own personal health information and with respect to appropriate collection, use and disclosure of their PHI and how they can address concerns about these things.

17. There should be comprehensive compulsory privacy training with appropriate privacy training materials for all QGH staff. This should include training on the Meditech system.

18. No employee should become an accredited user of Meditech unless there is evidence they have successfully completed the privacy training.

19. When any employee attempts to enter the Meditech system, the screen should display a caution against any collection, use or disclosure without a legitimate need for that employee to know the subject PHI.

20. The ‘reason to visit' should be a required field for any employee entering the Meditech system.

21. QGH should develop a masking option which would allow a patient to designate certain elements of their PHI not to be accessible without the patient's express consent.

22. The QGH should ensure that access to Meditech is closed immediately upon any employee no longer requires access whether by resignation, dismissal or change in position or for any other reason.

23. There should be a policy/procedure for suspending Meditech access privileges for anyone who has abused their user privileges.

24. The system should be configured so that it can randomly and pro-actively monitor access to the system and raise flags where anomalies are detected so that unauthorized access can be minimized.

25. That QGH develop a comprehensive policy for fax transmissions and the process when there are misdirected faxes.

26. That QGH ensure that fax machines are in secure areas of the facility not accessible to the general public.

27. That QGH develop an appropriate email/texting policy that specifically addresses personal information and personal health information

28. That QGH develop a mobile device policy for its employees, contractors and students that addresses both connecting with the Meditech system as well as the use of mobile devices brought into QGH by those individuals and utilized to collect PHI of patients. The 2003 COACH Guidelines provide an excellent set of security controls for mobile devices [p. 290]

29. That QGH ensure that any contracts that involve personal health information of patients of the QGH specifically identity what can and cannot be done with that PHI. All such contracts should explicitly incorporate by reference the privacy requirements imposed on any public body by ATIPPA.

30. That the QGH consider a checklist for non-consented disclosures of PHI to third parties:

    - Has the third party provided authority in writing of one of the 22 subsections of s. 48 of ATIPPA that might permit disclosure?
    - Is there authority in one of the 22 subsections of s. 48 of ATIPPA?
    - Is the request for disclosure properly documented so that the QGH has a record of the request?

- Is the purpose of the disclosure clear?
- Have steps been taken to ensure that the least amount of personal information which is necessary for that purpose is disclosed?
- Has QGH retained a record of the disclosure and relevant documentation?

31. That all staff working in Health Records, the clinics, OR and Emergency be made familiar with the two documents (Memo dated March 17, 2014 Disclosure of Personal Information to Law Enforcement and the Fact sheet: When the RCMP come to call).