Standing Committee on
Public Accounts, Independent Officers and Other Entities

Report on the Review of the Information and Privacy Commissioner's 2016 Report on the Privacy Audit of the Qikiqtani General Hospital

3rd Session of the 4th Legislative Assembly of Nunavut
Spring 2017 Sitting

Pat Angnakak, Chair
Alexander Sammurtok, Co-Chair
Tony Akoak, MLA
Joe Enook, MLA
David Joanasie, MLA
Pauloosie Keyootak, MLA
Steve Mapsalak, MLA
Simeon Mikkungwak, MLA
Paul Okalik, MLA
Emiliano Qirngnuq, MLA
Allan Rumbolt, MLA
Tom Sammurtok, MLA
Isaac Shooyook, MLA

www.assembly.nu.ca

Introduction

The *Access to Information and Protection of Privacy Act* provides for the Commissioner of Nunavut to appoint, on the recommendation of the Legislative Assembly, the Information and Privacy Commissioner for a five-year term of office.

Ms. Elaine Keenan Bengts was reappointed on February 24, 2015, for a 5-year term of office as Nunavut's Information and Privacy Commissioner. This is her fourth term as Information and Privacy Commissioner of Nunavut. Ms. Keenan Bengts also serves as the Information and Privacy Commissioner of the Northwest Territories.

The *Access to Information and Protection of Privacy Act* and regulations made under the Act were inherited from the Northwest Territories on April 1, 1999. Between 1999 and 2012, a number of minor amendments to the legislation were made to address conflicts with other territorial statutes.

Bill 38, *An Act to Amend the Access to Information and Protection of Privacy Act*, received 1st Reading on June 1, 2012. Bill 38 received Assent on June 8, 2012. These amendments provided clear authority for the Information and Privacy Commissioner to undertake privacy-related reviews concerning personal information held by public bodies. The amendments came into force on May 11, 2013.

In its *Report on the Review of the 2012-2013 and 2013-2014 Annual Reports of the Information and Privacy Commissioner*, which was presented to the Legislative Assembly on October 28, 2014, the standing committee recommended that "the Government of Nunavut co-operate with the Office of the Information and Privacy Commissioner in undertaking at least one formal privacy audit of a department, Crown agency or territorial corporation during the 2015-2016 fiscal year."

The Information and Privacy Commissioner's *Report on the Privacy Audit of the Qikiqtani General* was tabled in the House on November 8, 2016. The standing committee received a copy of the government's formal response to the Information and Privacy Commissioner's report on May 3, 2017, entitled *Department of Health Responses to IPC QGH Privacy Audit Recommendations* (Appendix A).

The May 10-11, 2017, appearances of the Information and Privacy Commissioner and Government of Nunavut officials before the standing committee took place in the Chamber of the Legislative Assembly. The standing committee's hearings were televised live across the territory and were open to the public and news media to observe from the Visitors' Gallery. Transcripts from the standing committee's hearings will be available on the Legislative Assembly's website.

Observations and Recommendations

Issue: Legislation and Policy

In her 2016 *Report on the Privacy Audit of the Qikiqtani General Hospital*, the Information and Privacy Commissioner recommends that the Government of Nunavut develop health-specific privacy legislation. The Information and Privacy Commissioner has been advocating for the development of this legislation for over a decade.

In its May 3, 2017, formal response to the recommendations of the Information and Privacy Commissioner, the government stated that:

> "Health is leading a Committee with representation from across the Department and Justice; the Committee is developing a legislative proposal (LP) as well as developing a list of privacy related activities that can be undertaken in the absence of legislation. It is anticipated that the legislative proposal will be submitted at the beginning of the next government."

The standing committee continues to encourage the department to work closely with the Information and Privacy Commissioner on the development of health-specific privacy legislation.

The standing committee is aware that it may be a number of years before health-specific privacy legislation is passed and brought into force in Nunavut. In the meantime, there are a number of outstanding issues concerning the protection of patients' privacy that the standing committee believes need to be addressed as soon as possible.

Section 42 of the *Access to Information and Protection of Privacy Act* mandates 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.

In her report, the Information and Privacy Commissioner describes various types of security arrangements and safeguards that can be implemented to achieve that goal. She states that:

> "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."

Unfortunately, in her report, the Information and Privacy Commissioner also states that:

> "What the Audit further revealed is that there is no privacy management program which is up-to-date, comprehensive and widely understood and supported. Without such a privacy management program, the efforts we did find to promote privacy awareness and compliance tend to be fragmented, inconsistent, and not well understood by all staff at QGH."

In her report, the Information and Privacy Commissioner indicates that, during the course of her site visit to the Qikiqtani General Hospital, she witnessed several cases where personal health information was being improperly collected and retained on the premises.

During the standing committee's May 10-11, 2017, televised hearing, government officials indicated that a number of procedures that are intended to ensure that personal health information is secured and protected are now being implemented. Some of these procedures include timed screensavers for the hospital's computers, newly secured offices with limited and electronic access, and the transfer of patient files from paper to electronic format.

The standing committee commends the hospital for its efforts. However, the standing committee is it is of the view that the hospital must develop and implement clear and comprehensive policies to ensure that all staff are adhering to those procedures and protecting patients' personal health information to the greatest extent possible.

The standing committee is aware that the government has implemented a number of policies concerning access to information and privacy, and has produced a comprehensive *Privacy Management Manual*, which may be accessed and used a resource by all government employees, including hospital staff. In its introduction, this Manual reads:

> "The Privacy Management Manual (PMM) is a comprehensive set of tools and resources to be used by all employees of the Government of Nunavut to successfully implement the privacy provisions of the Access to Information and Protection of Privacy (ATIPP) Act. All employees are required to familiarize themselves with the PMM as the ATIPP Act holds each employee accountable for the privacy of personal information under the custody and control of the government."

However, in her report, the Information and Privacy Commissioner stated that her office's audit "revealed very little familiarity with the Manual within QGH." She also stated that:

> "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."

During the standing committee's May 10-11, 2017, televised hearing, government officials did not provide much information on what, if any, privacy-specific policies and procedures are currently in place at the hospital. Government officials did provide some information on seven specific directives related to electronic health information, but these directives were, according to the Information and Privacy Commissioner, out-of-date and had not been implemented at the time of her audit.

During the standing committee's May 10-11, 2017, televised hearing, government officials testified that:

> "The question was for a list of the privacy…. I'm not sure on the exact wording, but the directives and the policies and so on. All of them are actually located in the report of the privacy commissioner. She had already included them in the appendix. The only thing that I would have to add to that is the privacy and security directives that guide employees, contractors and agents of the Government of Nunavut on matters concerning the management of e-Health systems, including the iEHR system and there are seven directives and I'll read them into the record. The seven directives include monitoring and audit of e-Health systems, e-Health information security, retention and disposal of electronic personal information, e-Health information privacy and password management for e-Health systems, collection use and disclosure of personal information in e-Health systems and finally e-Health access control. These are the directives that are being translated and will be tabled."

The standing committee is concerned that the department appears to only have prepared policies for personal health information that is collected, used and disclosed through its "e-Health systems," despite the fact that the hospital and community health centres are all operating on a hybrid system where personal health information is currently being retained in both paper and electronic formats.

While the standing committee recognizes that the Department of Health has made efforts to develop directives, policies and other materials to inform its employees of privacy best practices and expectations, these efforts need more coordination and monitoring.

Standing Committee Recommendation #1

The standing committee recommends that the Government of Nunavut provide, in its response to this report, a list of all formal policies that it currently has in place at the Qikiqtani General Hospital concerning the protection of privacy or access to information.

The standing committee further recommends that the Government of Nunavut develop a suite of policies that establish mandatory requirements and responsibilities for the protection of personal health information that is collected, used or disclosed by the hospital, community health centres, and all other health service providers in the territory.

The standing committee further recommends that the Government of Nunavut, in its work to develop privacy-specific policies for the hospital and community health centres, ensure that the following areas are addressed:

- A definition of personal health information;
- A limited list of persons who may receive access to personal health information;
- Training that will be required of persons who are provided with access to personal health information;
- Oaths of confidentiality or standards of conduct that must be acknowledged and agreed to by persons who may receive access to personal health information;
- A list of persons responsible for implementing privacy protection measures any and all guiding principles that must be acknowledged and agreed to by such persons;
- A list of the circumstances under which personal health information maybe accessed;
- Established procedures and processes that may be used to retain or destroy personal health information;
- Specific measures that will be taken to monitor the implementation of legislation and policies concerning privacy protection;
- Limits on the manner and scope that personal health information may be collected;
- Limits on the use, disclosure and retention of personal health information;
- A list of security safeguards that must be in place at each facility;
- An established process by which a person may access their information;

- Established procedures or processes by which health care service providers or the department must inform patients of their right to access their own personal health information;
- An established process by which a person can submit complaints and inquiries regarding their request to access their information;
- Established procedures and processes for addressing privacy incident and breaches specific to the hospital and community health centres;
- Established procedures or processes by which the hospital or community health centres will conduct privacy impact assessments; and
- Established rules for the agreements under which a health service provider may share personal health information, including the responsibilities of any third party service providers who receive access to personal health information under such agreements.

The standing committee further recommends that the Government of Nunavut provide, in its response to this report, a detailed timeline by which it plans to have completed a suite of comprehensive policies for the protection of personal health information.

The standing committee further recommends that the Government of Nunavut makes all policies related to the protection of personal health information available to the public as early as practicable.

Issue: Training

In order to implement or administer any privacy-related legislation or policy, the Department of Health ultimately relies on each individual employee in the hospital to understand and comply with appropriate practices and procedures concerning the collection, use and disclosure of personal health information.

In her report, the Information and Privacy Commissioner raises concerns that the department is not providing hospital staff with sufficient information or training on privacy best practices. In her report, the Information and Privacy Commissioner stated that:

> "We found that there is no comprehensive privacy training program for new hires nor in-service training on privacy best practices."

In her report, the Information and Privacy Commissioner recommended that:

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

In its May 3, 2017, formal response to the Information and Privacy Commissioner's report, the government did not clearly indicate if it agrees that comprehensive and privacy-specific training should be compulsory for all hospital staff. Instead, in response to this specific recommendation, the government only makes reference to "training on the Meditech system."

During the standing committee's May 10-11, 2017, televised hearing, government officials did provide some information on the training that it is currently provided to hospital staff to inform them of privacy best practices and of their obligations under the *Access to Information and Protection of Privacy Act*. During the standing committee's televised hearing, the following exchange took place:

> "Mr. Rumbolt: Thank you, Madam Chairperson. One final question. On page 41 of the report, the Information and Privacy Commissioner states that she found stacks of patient files sitting on unattended desks during the course of her audit. What types of training does your department provide to hospital staff to inform them of privacy best practices? Thank you, Madam Chairperson.
>
> Chairperson: Thank you, Mr. Rumbolt. Ms. Stockley.

> Ms. Stockley: Thank you, Madam Chairperson. Again, it's an on-the-job type of training that is provided on orientation with periodic updates through directives coming from the department, newsletters, and updates shared with staff. Thank you, Madam Chairperson."

During the standing committee's May 10-11, 2017, televised hearing, government officials also testified that:

> "Health provides periodic communications to its staff such as ATIPP coordinator guides on topics such as proper encryption of confidential information, sending and receiving electronic and physical mail, and how to properly save files to protected drives. Information related to privacy protection is also disseminated though interdepartmental newsletters. Staff training opportunities around records management and ATIPP training are available and provided by the Government of Nunavut, as well as through presentations offered to community health staff groups during meetings and conferences."

During the standing committee's May 10-11, 2017 televised hearing, government officials also testified that:

> "We do regular circulation of privacy directives for staff and the expectation is that they will inform their patients, their clients. We do consistent training and presentations for all staff. We do standard orientation presentations for new frontline health care providers, and we do information dissemination through the two health internal newsletters called *The Pulse* and *The Connection* that are distributed right throughout the territory to health care providers."

The standing committee is concerned that the training described by government officials is not sufficient to constitute comprehensive and privacy-specific training, for a number of reasons.

First of all, there appears to be no expectation that **all** hospital staff should have **privacy-specific** training. The official's testimony that the department does provide "consistent training and presentations for all staff" was not supplemented by any clear description of what components are included in that training. The official's testimony that "standard orientation presentations [are provided] for new frontline health care providers" does not explicitly confirm that this "orientation presentation" includes clear and specific information related to privacy best practices.

Secondly, if not all staff are required to take privacy-specific training at this time, there still appears to be no clear policy, directive or guideline that specifies **which** hospital staff must have **privacy-specific** training.

Furthermore, in their testimony, government officials made no mention of any mechanism to track whether or not staff who are required to take privacy-specific training do, in fact, take that training.

The standing committee recognizes that the Department of Health makes efforts to provide ATIPP training to hospital and community health centre staff. However, in the same way that the *Access to Information and Protection of Privacy Act* does not provide the necessary health-specific legislative framework that the territory needs, the standing committee is of the view that the related ATIPP training does not provide the specific information that hospital and health centre staff need to know in order to protect the patients' privacy to the greatest extent possible.

The standing committee is also concerned about the department's apparent reliance on the use of presentations and "information dissemination" in providing information and training on privacy best practices to hospital staff. Presentations do not measure the extent to which an individual is knowledgeable about a particular subject and while information dissemination, in forms such as newsletters, may be informative, it is difficult to determine if the information disseminated is in fact being absorbed and used by the intended audience.

While the standing committee commends the Department of Health for its efforts to inform and train hospital staff of privacy best practices, it agrees with the Information and Privacy Commissioner that a comprehensive and privacy-specific training program needs to be developed for all hospital and community health centre staff.

The standing committee is of the view that without comprehensive and privacy-specific training for all staff, it will be very difficult for the hospital and community health centres to confidently assure their patients that they are equipped to protect personal health information.

Standing Committee Recommendation #2

The standing committee recommends that the Government of Nunavut develop a comprehensive training program for hospital and community health centre staff that includes, but is not limited to, the following components:

- Information and procedures related to the patient's right to access;
- Information and procedures related to identifying and reporting privacy breaches and incidents;
- A specific list of individuals that staff may contact with concerns related to privacy protection in the hospital;
- Implementing privacy best practices in the workplace, including,
    - Storing, transferring and destroying paper and electronic files,
    - Use of email, fax, mobile and other electronic devices,
    - Having conversations in open spaces, and
    - Sharing information with third parties;
- Detailed training on all relevant policies, directives and procedures that may be in place at the facility at that time.

The standing committee recommends that the Government of Nunavut provide, in its response to this report, a detailed timeline by which it plans to complete this comprehensive training program.

The standing committee recommends that the Government of Nunavut make the above-mentioned training program compulsory for all employees who may have access to personal health information that is used, collected, or disclosed by the Government of Nunavut.

The standing committee recommends that the Government of Nunavut implement a system to track and monitor all privacy-specific training that is provided to staff, including any training related to the use of Meditech.

Issue: Oversight

The presence of privacy-specific training programs and policies alone will not be sufficient to ensure that adequate safeguards are in place to protect patients' privacy. These privacy training programs, policies and all other efforts will need to be focused, coordinated and monitored before privacy best practices are implemented at the hospital in a thorough and consistent manner.

In her report, the Information and Privacy Commissioner recommended that the department appoint a Privacy Officer, who will have a designated leadership role in privacy compliance efforts within the hospital. This Privacy Officer should also have the mandate to develop a comprehensive privacy management program, providing advice on privacy compliance to the regional and community health centres. The Information and Privacy Commissioner also recommended that this Privacy Officer be responsible for:

- Providing input on achieving good privacy compliance in new programs, new software and policies for the hospital and community health centres;
- Developing a full suite of written policies and procedures for privacy compliance;
- Overseeing staff privacy training for all new hires, in-service training for existing employees, as well as volunteers and contractors;
- Ensuring that all out-sourcing contracts that involve significant volumes of personal health information include the necessary privacy protections; and,
- Ensuring that patients are made aware of their privacy rights.

The standing committee agrees with the Information and Privacy Commissioner's recommendation and emphasises that the department must make every effort to ensure that the above-mentioned responsibilities are being fulfilled, even in the absence of a formal privacy officer.

During the standing committee's May 10-11, 2017, televised hearing, government officials supplemented that response and testified that:

> "While we agree with that, we actually had a privacy officer position. It went out for competition and was never successful in being filled. I believe the first time it went out for competition was in 2011. Instead of having nobody to do it, we now have two positions that share responsibilities for the job that one person would do in many other jurisdictions. That is how we have tried to do what we could here in our territory. We have the responsibility for privacy divided between two positions. One is a clinical adviser and one is a quality assurance and risk management coordinator. I'm happy to say both of those positions are filled."

The standing committee recognizes that it may be a number of years yet before the department successfully fills a privacy officer position. The standing committee encourages the department to identify a specific position or position(s) that will be responsible for providing that focus, coordination and monitoring until such a time as a privacy officer is appointed at the hospital.

Standing Committee Recommendation #3

The standing committee recommends that the Government of Nunavut provide**, i**n its response to this report, a detailed timeline by which the department plans to open a privacy officer position for competition.

The standing committee recommends that the Government of Nunavut provide, in its response to this report, a detailed listing of the specific positions that will be responsible for each of the following tasks within the hospital and community health centres:

- Leading privacy compliance efforts;
- Developing a comprehensive privacy management program;
- Providing advice on privacy compliance to the regional and community health centres;
- Providing input on achieving good privacy compliance in new programs, new software and policies for the hospital and community health centres;
- Developing a full suite of written policies and procedures for privacy compliance;
- Overseeing staff privacy training for all new hires, in-service training for existing employees, as well as volunteers and contractors;
- Ensuring that all out-sourcing contracts that involve significant volumes of personal health information include the necessary privacy protections; and,
- Ensuring that patients are made aware of their privacy rights.

Department of Health Responses to IPC QGH Privacy Audit Recommendations

IPC Recommendation #1:

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

Health Response: QGH (as all Health Centres) is not a stand-alone entity, but rather reports to the Deputy Minister of Health through the Assistant Deputy Minister, Operations. Therefore, it is a public body under the oversight of the Department of Health and subject to the *ATIPPA*. If the Government of Nunavut should, in the future, establish Health Authorities with separate Governance Authorities, this recommendation could be revisited and applied to all health care facilities in the territory, as governed by applicable legislation.

IPC Recommendation #2:

That the GN develop a stand-alone health information law similar to such laws in other Canadian jurisdictions.

Health Response: Health is leading a Committee with representation from across the Department and Justice; the Committee is developing a Legislative Proposal (LP) as well as developing a list of privacy related activities that can be undertaken in the absence of legislation. It is anticipated that the legislative proposal will be submitted at the beginning of the next government.

The Committee is currently working to develop a culture of privacy within the Department of Health through the following activities:

- regular circulation of privacy directives for staff;
- consistent training and presentations for all staff;
- standard orientation presentations for new front-line health care providers; and
- information dissemination through the Pulse and the Connection (Health's internal newsletters).

IPC Recommendation #3:

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.

Health Response: A jurisdictional scan was completed by the Committee on specific privacy legislation with the aim of implementing legislation that is accessible and appropriate for Nunavut.

IPC Recommendation #4:

That QGH appoint a Privacy Officer with the following features:

1. *Designated leadership role to lead the privacy compliance efforts in QGH;*
2. *Sufficiently senior to be able to have ready access to the CEO and senior management;*
3. *Mandated to develop a comprehensive privacy management program;*
4. *To provide input to the CEO and senior management on achieving good privacy compliance in new programs, new software and policies;*

5. *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;*
6. *To ensure proper privacy protection in out-sourcing contracts that involve significant volumes of personal health information;*
7. *To be the key liaison between the QGH and the Office of the Information and Privacy Commissioner;*
8. *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;*
9. *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.*
10. *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.*

Health Response: The Department will give this recommendation serious consideration as it develops and implements Health Specific Privacy legislation. The responsibility for privacy at QGH is divided between the Clinical Advisor (CA) and the Quality Assurance and Risk Management Coordinator (QARM). The Clinical Advisor is accountable for the development of policy, procedures, practices, and guidelines for IHS. The CA is also accountable for the development of educational material related to privacy. The QARM is accountable for the Quality, Safety, and Risk piece, which includes the reporting, analysis, review, capture, and reporting of events (near misses, incidents, and sentinel events), as well as disclosure. As part of this process, Iqaluit Health Services is currently working on the development of a monthly events reporting and analysis report, which will provide an overview of all events, and will designate privacy breaches as a separate item on the report. The ATIPP manager and ATIPP Coordinator will be involved to ensure these processes are consistent with legislation and already established protocols.

IPC Recommendation #5:

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

Health Response: The implementation of an electronic incident reporting system will not be pursued until such time as the Quality Improvement (QI) Unit is staffed. The preliminary work prior to the implementation of an electronic system will require the review, revision & stream lining of the paper based incident reporting system & developing the business processes to support this implementation. Iqaluit Health Services is currently tracking all breaches as part of our events reporting and analysis process. This means that privacy breaches are reported, analysed, reviewed, and captured along with all other near misses, events, incidents, sentinel events, etc. Please also see note under item #4 for more information on planned next steps.

IPC Recommendation #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.

Health Response: Health agrees with the need to further develop privacy management programming and has already commenced this initiative. The Department wants to achieve a system that will address the territorial health system, including QGH.

IPC Recommendation #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 way 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.

Health Response: As noted under recommendation #4, the responsibility for privacy at QGH is divided between the Clinical Advisor (CA) and the Quality Assurance and Risk Management Coordinator (QARM). The Clinical Advisor is accountable for the development of policy, procedures, practices, and guidelines for Iqaluit Health Services. The CA is also accountable for the development of educational material related to privacy. The QARM is accountable for the Quality, Safety, and Risk piece, which includes the reporting, analysis, review, capture, and reporting of events (near misses, incidents, and sentinel events), as well as disclosure. As part of this process, Iqaluit Health Services is currently working on the development of a monthly events reporting and analysis report, which will provide an overview of all events, and will designate privacy breaches as a separate item on the report. The ATIPP manager and ATIPP Coordinator will be involved to ensure these processes are consistent with legislation and already established protocols. The Department is exploring possible protocols within the Office of Patient Relations as per this recommendation.

IPC Recommendation #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.

Health Response: The Department of Health and Department of Community and Government Services have in place a comprehensive plan. Close to 50% of EMR roll-out has been completed and the remainder is anticipated to occur by the end of December 2017.

IPC Recommendation #9:

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

Health Response: Health concurs that this must be an important practice and standard. Health is committed to conducting an assessment of current practice to identify gaps and best practices.

IPC Recommendation #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.

Health Response: Health will commit to review current practices, identify gaps and areas for improvement.

IPC Recommendation #11:

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

Health Response: Health does not currently have a clean desk policy for QGH. Health will review the current policies and ensure that this item is captured. Health will also review screen lock/current time out within Health Centres and QGH. This will also assist in protecting patient files.

IPC Recommendation #12:

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

Health Response: Health supports this recommendation and will follow-up on this recommendation to ensure safeguards are in place to limit access. The Health Information Management Office (previously Health Records) has developed an office access protocol. Access to the office is controlled by an access card, and an access rights list has been developed. Employees of the Health Information Management Office and Iqaluit Health Services Senior Leaders (Executive Director and Directors), as well as Nursing Managers, have access to the office to ensure due diligence in protecting the information, while allowing for access to the information when it is necessary for the purposes of the delivery of care.

IPC Recommendation #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.

Health Response: Health will commit to reviewing and evaluating this recommendation.

IPC Recommendation #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.

Health Response:

- The Department of Health and Department of Community and Government Services have in place a comprehensive plan. Close to 50% of EMR roll-out is complete and the remainder is anticipated to be finalized by the end of December 2017.
- A PIA and TRA was completed prior to implementing MEDITECH. Health intends to update the PIA and TRA prior to the end of 2017. Results of these assessments will be appended to the original documents.
- The iEHR steering committee will review and evaluate the recommendation to address EHR conversion from paper to digital format.

IPC Recommendation #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.

Health Response: The Department will consider this recommendation and how it can apply this initiative across the territory to include QGH.

IPC Recommendation #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.

Health Response: This initiative is currently being addressed through the Department's review of its patient relations division, the creation of the Continuous Quality Improvement (CQI) unit and requirements as part of developing Health Specific Privacy Legislation.

IPC Recommendation #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.

Health Response: Please see response under recommendation #8.

IPC Recommendation #18:

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

Health Response: This recommendation is addressed through our current training program.

IPC Recommendation #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.

Health Response: The Department agrees with this recommendation and has commenced its work with MEDITECH and our Healthtech to complete this work. It will become a standard message.

IPC Recommendation #20

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

Health Response: This is a requirement on the registration screen; however Health will review the current format to ensure protection of client privacy.

IPC Recommendation #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.

Health Response: This is a business solution that is available within Meditech. Health agrees with this recommendation and will initiate the process to establish an appropriate policy.

IPC Recommendation #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.

Health Response: Currently when an employee leaves the employment of the GN, an employee clearance form is submitted to Community and Government Services. Once submitted, GN-Health access is terminated and the employee can no longer access MEDITECH. Once web-based Ambulatory is introduced, Health will also include a Health IT clearance form that will trigger the same actions when an employee no longer is employed by the GN-Health.

IPC Recommendation #23:

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

Health Response: Currently, MEDITECH access can be suspended at the request of either a Manager/Director. We agree with this recommendation and Health will move to formalize this process with the development of a Health IT policy.

IPC Recommendation #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.

Health Response: Health agrees with this recommendation and Health IT is currently working with Healthtech Consultants to assist Health IT with the development of the requirements and procurement of an auditing tool for EHR.

IPC Recommendation #25:

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

Health Response: Health will review and evaluate current policy to identify gaps and take steps to address this recommendation. The events reporting and analysis process, which is the same process that is used to identify, analyze, track, and respond to all potential incidents also applied to misdirected faxes. As such, when a misdirected fax is reported, it is treated like any other event that potentially constitutes an incident, and is handled in the exact same manner.

IPC Recommendation #26:

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

Health Response: Health is in agreement and will implement a plan to effect this requirement. The Department has evaluated the location of all fax machines at QGH. It was determined that one fax machine was not in compliance, and the team is currently working on placing the said fax machine in a location that will ensure security of the information.

IPC Recommendation #27

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

Health Response: Health will review and evaluate current policy to identify gaps and take steps to address this recommendation.

IPC Recommendation #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]

Health Response: Health will review and evaluate current policy to identify gaps and take steps to address this recommendation.

IPC Recommendation #29:

That QGH ensure that any contracts that involve personal health information of patients of the QGH specifically identify 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.

Health Response:

- "Health & Medical Record "is currently in all contract details outlining the type of records and its protection. Patient Identification is also addressed, as well as the exchange of information.
- Confidentiality clauses are in all GN contracts to include Health. The Department will request a review of all contracts to ensure they reference the privacy requirements as imposed by ATIPPA.

IPC Recommendation #30:

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

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

Health Response: Health agrees with this recommendation and will conduct a review and develop a checklist that can be used across the territory and with QGH.

IPC Recommendation #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).

Health Response: Health will implement this request.