Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE		
	iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
Monitoring and Audit of eHealth Systems Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			3
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) on matters concerning the monitoring and audit of users and external agents who access eHealth systems.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Section 42 of ATIPP requires Health to protect personal information (PI) "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

2. PRINCIPLES

1. Health shall monitor and audit access to eHealth systems in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to protect PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
    d. Access to eHealth systems is for authorized purposes only.
    e. The GN has the right and duty to monitor and audit user access to eHealth systems to ensure that PI is collected, used and disclosed only for authorized purposes.

f. The GN has the responsibility to protect the confidentiality, integrity and availability of PI and other eHealth system assets.

3. SCOPE AND APPLICABILITY

This Monitoring and Audit of eHealth Systems Directive applies to:

1. All users including employees, contractors, and agents of the GN and all vendors and suppliers of products and services to the GN who access, use, operate and/or support eHealth systems.
2. All eHealth and associated system assets including:
    a. Sensitive data that includes:
        i. PI;
        ii. System audit logs; and
        iii. System and security administration data (e.g. technical security configurations, authentication and password data);
    b. Hardware, including mobile devices and tele-networking equipment;
    c. Software; and
    d. Network and communications resources.

4. ROLES AND RESPONSIBILITIES

1. The Health Information Division (HID) for Health is responsible for monitoring and auditing user access to PI in eHealth systems.
2. The Security Officer for the Department of Community and Government Services (CGS) is responsible for monitoring and auditing eHealth systems to detect and respond to unauthorized access by external agents (e.g. hackers) that may compromise the confidentiality, integrity and availability of PI and eHealth system assets.

5. AUDIT LOGGING

1. The HID and CGS will enable audit logging functionality in all eHealth systems.
2. The HID and CGS will define audit reports to be generated by eHealth systems based on the risk of unauthorized access, collection, use and disclosure of PI, or risk to the confidentiality, integrity and availability of eHealth system assets determined by any Threat and Risk Assessment (TRA).

6. MONITORING AND AUDIT PROGRAM – ACCESS BY USERS

1. The HID will establish a program to audit user access to eHealth systems to ensure that PI and eHealth systems are used in an appropriate manner by authorized users.
2. The HID will establish criteria for identifying potential privacy and security breaches based on threats defined in any Privacy Impact Assessment (PIA) or TRA, or identified as a result of the ongoing implementation of the program. Criteria may include, but is not limited to:
    a. Access to the health records of VIPs, family members or friends of employees of Health;
    b. Access to health records that contain PI related to communicable diseases, sexually transmitted infections, HIV/AIDS test results, substance abuse, mental health and other highly sensitive information;
    c. Access to health records from home or other remote locations; and
    d. Access to health records at unusual times (e.g. in the middle of the night).
3. Where it is suspected that a user has accessed PI for purposes not related to their role or job function, the HID will alert Health's ATIPP Coordinator.

4. The ATIPP Coordinator will investigate the situation and may request that an audit on all accesses to PI and eHealth systems by the user be conducted by the HID to determine whether or not a breach has occurred in accordance with ATIPP and the Privacy Breach and Incident Policy.
5. The ATIPP Coordinator will investigate all cases where it is suspected that a privacy breach may have occurred.
6. Where it is determined that a privacy breach may have occurred, the ATIPP Coordinator will initiate the privacy breach protocol defined in ATIPP and the Privacy Breach and Incident Policy.

7. MONITORING AND AUDIT PROGRAM – EXTERNAL AGENTS

1. CGS will establish a program to monitor and audit all unauthorized access to eHealth systems by external agents outside of the GN infrastructure.
2. CGS will establish criteria for identifying potential security breaches based on threats defined in any TRA or identified as a result of the ongoing implementation of the program.
3. CGS will investigate all cases where it is suspected that security breach may have occurred based on the defined criteria.
4. Where it is determined that a security breach may have occurred, CGS will notify the ATIPP Coordinator who will initiate the privacy breach protocol defined in ATIPP and the Privacy Breach and Incident Policy.

8. ADMINISTRATION OF THIS DIRECTIVE

This directive will be reviewed on an annual basis by the Deputy Minister of CGS and Deputy Minister of Health or immediately upon commencement of any privacy or security breach investigation related to the monitoring or auditing of eHealth systems or a negative finding in a TRA or security audit. A report of such review will be provided to the Minister of CGS and Minister of Health.

9. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

_____ _____

Deputy Minister
Department of Community and Government Services

Date

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
eHealth Information Security Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			4
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN), on the management of information security associated with eHealth initiatives, including the interoperable Electronic Health Record (iEHR) system.

The Department of Health (Health) relies upon the confidentiality, integrity, and availability of information and technology-based systems to provide client care and to manage the delivery of health services. It is essential that GN information and technology-based systems are continuously protected and utilized in a secure and controlled manner.

Health is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Section 42 of ATIPP requires Health to protect personal information (PI) "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

This eHealth Information Security Directive is supported by topic-specific directives, standards, and operating procedures.

2. PRINCIPLES

1. eHealth systems will be deployed and operated in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).

c. The GN, which includes Health, has a statutory obligation to protect PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
d. All employees, contractors and agents of the GN are responsible for safeguarding the privacy and confidentiality of PI processed by and/or stored in eHealth systems, whether created by the GN or entrusted to the GN by clients, health care providers, or other sources.
e. Strategies, policies, and standards for managing information security in eHealth systems must be closely coordinated and integrated with the vision, objectives, and plans of the GN.
f. eHealth system users must be aware of their responsibilities for the security and privacy of PI and technology-based systems, and they must know what they can and must do to maintain security.
g. eHealth system users must act in a timely and co-operative manner to prevent, detect, and respond to security incidents.
h. Information security risks must be analyzed, treated, and monitored. Senior management must take reasonable action to manage information security risks.
i. The security of eHealth systems and networks must be reviewed and reassessed at regular intervals so that appropriate modifications to security policies, directives, standards, safeguards, and procedures can be made.

3. SCOPE AND APPLICABILITY

1. This eHealth Information Security Directive applies to:
    a. All users of eHealth systems including employees, contractors and agents of the GN who access, use, operate and/or support eHealth systems.
    b. All eHealth information system assets including PI in electronic format, system administration and security data, hardware, software and communications networks and facilities.
    c. All activities associated with the installation and operation of eHealth systems.

4. ROLES AND RESPONSIBILITIES

1. The Deputy Minister of Health:
    a. Is responsible for the administration of all provisions pursuant to this directive; and
    b. Shall issue topic-specific directives relating to eHealth systems, as required.
2. The Department of Health:
    a. Is accountable and responsible for information security in eHealth systems;
    b. Shall establish and maintain an Information Security Management Program;
    c. Shall develop and maintain an eHealth Information Security Directive and associated topic-specific directives and operating procedures for eHealth systems; and
    d. Is responsible and accountable for the day-to-day application of reasonable security management measures to protect against the unauthorized access, collection, use, disclosure, retention or disposal of PI, and for ensuring the availability of eHealth systems.
3. The Department of Community and Government Services (CGS):
    a. Is responsible for the implementation of reasonable physical and logical security measures to protect eHealth systems, associated systems and communications networks housed in GN facilities or contracted by CGS to third parties;
    b. Shall ensure that eHealth systems are configured and maintained in accordance with legislation, security policies, directives, standards and procedures;

c. Shall monitor eHealth systems for attacks by internal or external agents;
d. Shall ensure that necessary safeguards to protect eHealth systems against threats identified in any Threat and Risk Assessments (TRA) are implemented;
e. Is responsible for developing, testing and maintaining a disaster recovery plan to ensure minimal disruption to health services in the event of a catastrophic system failure;
f. Is responsible for detecting, investigating and responding to security breaches; and
g. Is responsible for identifying, evaluating, and documenting all eHealth system assets, including PI, systems administration and security data, hardware, software, and communications facilities; and, in consultation with Health, assign levels of sensitivity, criticality and ownership to them.

4. Users of eHealth systems:
    a. Are responsible for maintaining the confidentiality of PI, for following all security policies, directives and procedures; and for reporting any security incidents or suspected security incidents.

5. INFORMATION SECURITY MANAGEMENT PROGRAM

1. The Information Security Management Program will include the following components:
    a. Maintenance of a Threat and Risk Assessment program for eHealth systems and for managing risks identified through such program.
    b. Provision of privacy and security awareness training to all users of eHealth systems.
    c. Monitoring and audit of access to eHealth systems and compliance with this eHealth Information Security Directive and topic-specific directives.
    d. Participation with CGS in the investigation and response to security incidents, including unauthorized access attempts or attempts to compromise an eHealth system.
    e. Monitoring and reporting on the status of the information security program to senior management.
    f. Provision of ongoing guidance to users on matters related to information security.
    g. Definition of security requirements for services provided by organizations (program partners) that support eHealth systems, and monitoring to ensure compliance with those requirements, policies and directives.
    h. Establishment of agreements with suppliers and vendors of products and services, ensuring that suppliers and vendors comply, as required, with this eHealth Information Security Directive, topic-specific directives, standards and operating procedures.
    i. Development, testing and maintenance of a business continuity plan for each eHealth system to ensure continued delivery of health services in the event of a system failure.
    j. Determination and classification of the sensitivity of PI in eHealth systems and ensuring that adequate security safeguards commensurate with the sensitivity of the PI are implemented.

6. ACCESS TO EHEALTH SYSTEMS

1. eHealth systems will apply role-based access control.
2. Role definitions for users and operators will be defined by Health in consultation with stakeholders. Users and operators will be assigned roles by their managers.
3. Access to eHealth systems will be granted on a need-to-know basis, based on the user's role.
4. All user activity, including access to eHealth systems, is subject to monitoring and audit by Health.

7. VIOLATIONS

1. Any violation of this eHealth Information Security Directive, or any related topic-specific directives, standards and operating procedures by an employee of the GN is subject to the disciplinary policies and procedures of the GN.
2. Any violation of this eHealth Information Security Directive, or any related topic-specific directives, standards and operating procedures by a supplier, vendor or contactor or their respective employees and agents, is subject to remedies identified in the agreement or contract. Health or CGS may request the removal of a supplier, vendor or contractor or their respective employees and agents upon the occurrence of any such violation.

8. ADMINISTRATION OF THIS DIRECTIVE

1. This directive will be reviewed on an annual basis by the Deputy Minister of Health or immediately upon the occurrence of any security breach investigation related to the unauthorized collection, use or disclosure of PI or negative finding in a TRA or audit. Topic-specific directives will also be reviewed upon the occurrence of a security breach as applicable given the nature of the breach. A report of such review will be provided to the Minister of Health.

9. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

_____ _____

Deputy Minister
Department of Community and Government Services

Date

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE	
	iEHR PRIVACY AND SECURITY DIRECTIVE	
TITLE:	**SECTION:**	**POLICY NUMBER:**
Retention and Disposal of Electronic Personal Information Directive		
EFFECTIVE DATE: / **REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
		4
APPLIES TO:		
All employees, contractors, and agents of the GN who use eHealth systems		

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) on matters concerning the retention and disposal of personal information (PI) held in electronic form.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Section 42 of ATIPP requires Health to protect PI "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

2. PRINCIPLES

1. Health shall retain and dispose of PI in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
    d. PI in electronic form shall be retained in conformance with the requirements of the Archives Act and ATIPP.
    e. PI in electronic form shall be retained for a period appropriate to the purposes for which the information was collected.
    f. PI will be destroyed or made anonymous after the defined retention period has expired in accordance with the requirements of the Archives Act.

g. Media containing PI that is no longer required will be destroyed in a complete and secure manner.

3. SCOPE AND APPLICABILITY

1. This Retention and Disposal of Electronic Personal Health Information Directive applies to:
    a. All employees, contractors, and agents of the GN, and all vendors and suppliers of products and services to the GN, who access, use, operate and/or support eHealth systems.
    b. All PI held in an electronic format. This includes production data (i.e. data in active records), archived data, backup copies of the data created for disaster recovery and business continuity purposes, audit logs that contain PI, and copies of data created for other authorized purposes.
    c. All application software and security critical system data required to read PI stored in electronic formats.

4. ROLES AND RESPONSIBILITIES

1. The Public Records Committee for the GN has overall accountability for approving retention schedules and methods of disposal for public records under the authority of the Archives Act.
2. Primary accountability and responsibility for the retention and disposal of PI held in electronic format in eHealth systems rests with Health.
3. The Department of Community and Government Services (CGS) maintains the responsibility for the security of PI retained in systems and facilities; including the secure destruction and disposal of PI and media containing PI.

5. RETENTION OF PI

1. In accordance with Records Disposition Authority (RDA) 2005-3, PI in electronic form will be retained for a period of 20 years following the date of the last entry, the date of death of the individual, or the date of reaching age of majority. This does not apply to backup copies of PI databases created for disaster recovery and business continuity purposes and for audit logs that contain PI.
2. Health and CGS will establish retention schedules for backup copies of PI databases created for: disaster recovery and business continuity purposes; audit logs that contain PI; and copies of data created for other authorized purposes. This will be done in accordance with RDA 1995-32, Revised 2007-01 (Administrative Records Classification System). These schedules will be based on an assessment of business requirements.
3. Health will maintain an inventory of all databases and repositories of PI held in electronic form, including backup copies created for disaster recovery and business continuity purposes, audit logs that contain PI, and copies of data created for other authorized purposes.
4. Users will not copy or download PI from eHealth systems without authorization from Health. Health will establish an agreement with users who download data for authorized purposes and will maintain a record of the data downloaded, its location, the contact person responsible for safeguarding the data and conditions for retention and disposal of the data.
5. CGS will ensure that any software, hardware or utilities (e.g. encryption programs) required to read or copy archived or backed-up PI is available for the entire period that the PI is retained.
6. When there is a change in technology (e.g. new version of software), CGS will ensure that the new technology can read production and archived data. In the event that the new

technology is unable to read production and archived data, CGS will convert the data into a format that can be read by the new technology.
7. If data is stored in an encrypted format, CGS will ensure that the encryption programs, algorithms and keys required to decrypt production and archived data will be available during the entire retention period, and will be retained in a secure environment.
8. Health and CGS will establish appropriate controls to protect PI from loss, destruction and falsification to ensure compliance with this directive.

6. BACKUP AND BACKUP RETENTION

1. Health and CGS will establish a data backup schedule to ensure that data is available for disaster recovery purposes.
2. The disaster recovery plan will provide details of the data required to be stored in backup form in order to recover from a disaster, including PI, application software and security critical system data.
3. Media containing backup data will be stored in a secure location separate from the primary storage site (e.g. away from the production data and archived data).
4. Following secure deletion of the data previously stored on the media, magnetic tapes and other media containing backups of data, including PI, application software, and security critical system data, such media may be recycled and reused. Health and CGS will determine and will document in procedures, the method(s) for sanitizing backup media.

7. DISPOSAL AND DESTRUCTION OF PI

1. At the end of the retention period, PI and any copies of the PI that are no longer required for the purposes for which it was collected, will be destroyed or rendered anonymous.
2. In collaboration with CGS, Health will obtain written authority from the Public Records Committee prior to destroying or disposing of any electronic records containing PI.
3. Where PI is rendered anonymous, an effective anonymization or pseudonymization algorithm and program will be applied. After anonymization or pseudonymization is completed, the source files will be destroyed in a secure manner.
4. Health and CGS will determine and document in procedures, the method(s) for destroying or permanently erasing media containing PI, application software, or security critical system data.
5. When media containing PI, application software, or security critical system data is no longer required, the media will be destroyed in a complete and secure manner or permanently erased.
6. Before equipment or devices that include media containing PI, application software, or security critical system data are sent out for repair, reuse or disposal (e.g. hard drives, flash drives) media containing such data will be permanently removed, destroyed or erased.

8. ADMINISTRATION OF THIS DIRECTIVE

This directive will be reviewed on an annual basis by the Deputy Minister of CGS and Deputy Minister of Health or immediately upon commencement of any security breach investigation related to the retention or disposal of PI; or a negative retention or destruction control finding in a Threat and Risk Assessment or security audit. A report of such review will be provided to the Minister of CGS and the Minister of Health.

9. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

_____ _____

Deputy Minister
Department of Community and Government Services

Date

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE		
	iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
eHealth Information Privacy Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			5
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) for the protection of personal information (PI) associated with eHealth initiatives, including the interoperable Electronic Health Record (iEHR) system.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), a law established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health Information (PHI).

Clients expect and trust that the GN will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

This eHealth Information Privacy Directive is supported by topic-specific directives, standards, and operating procedures.

2. PRINCIPLES

1. eHealth systems will be deployed and operated in conformance with the following principles:
    a. The priority of strengthening the public services will be advanced by eHealth infrastructure, which provides improved, efficient and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to protect PI under its control by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of such PI.
    d. Every individual has a basic need for privacy and legal right to have control over the collection, use and disclosure of their PI.
    e. PI shall be collected, used and disclosed only by authorized individuals in accordance with ATIPP, other applicable legislation, the GN's policies, and Health's policies and directives respecting the privacy and security of PI.

3. SCOPE AND APPLICABILITY

1. This eHealth Information Privacy Directive applies to:
    a. All employees, contractors, and agents of the GN who access, use, operate and/or support eHealth systems.
    b. All PI collected, used, disclosed, and retained by the GN in association with eHealth systems.

4. ACCOUNTABILITY

1. The Minister of Health:
    a. Under ATIPP, has delegated authority to the Deputy Minister of Health for all collection, use and disclosure of PI. Accordingly, the Deputy Minister of Health is responsible for the administration of all provisions pursuant to this directive.
2. The Deputy Minister of Health:
    a. Shall establish and maintain an Information Privacy Program;
    b. Shall develop and maintain topic-specific directives and operating procedures for eHealth systems;
    c. Is accountable and responsible for the protection of PI accessed, collected, used, disclosed, stored and retained in relation to eHealth systems, whether created by Health or entrusted to Health by clients, health care providers, or other sources; and
    d. Shall ensure that all agents to whom Health has transferred PI to for processing or handling are bound by contractual means to provide a comparable level of protection while such PI is being processed or handled.
3. eHealth System Users:
    a. Are responsible for safeguarding the privacy and confidentiality of PI collected, used, and disclosed in the course of their duties at all times; and
    b. Must act in a timely and co-operative manner to prevent, detect, and report privacy breach incidents.

5. IDENTIFIED PURPOSES

1. When collecting PI directly from a client, Health shall identify the purposes for which PI is collected, used and disclosed and the specific legal authority for the collection of the PI. Health shall also inform the client of the title, business address and telephone number of the person who can answer questions about the collection, use, disclosure, and retention of the individual's PI in relation to eHealth systems.
2. Health shall not use PI for any other purpose than an identified purpose and will require the express written consent of the client if a new purpose is not authorized by legislation.

6. CONSENT

1. Where ATIPP requires consent of the client for collection, use or disclosure of PI, such consent must be in writing or given orally and must specify to whom the PI may be disclosed and how the PI may be used. The consent must also be knowledgeable, in that it should be reasonable in the circumstances to believe that the client knows:
    a. The purpose for the collection, use or disclosure; and
    b. That the client may give or withhold their consent.
2. Where the consent required under subsection 1 above is given orally then Health shall, as soon as reasonably possible, create and retain a written record of such consent.

7. LIMITING COLLECTION

1. Health shall not collect PI indiscriminately. Both the amount and type of information collected will be limited to that which is necessary to fulfill the purposes identified.
2. PI shall be collected only by lawful means. Clients shall not be misled or deceived about the purposes for which the information is being collected.

8. LIMITING USE, DISCLOSURE AND RETENTION

1. PI shall not be used or disclosed for purposes other than those for which it was collected or for a use consistent with that purpose, except with the express consent of the client.
2. PI that is no longer required to fulfill the identified purposes shall be destroyed or made anonymous. Subject to any legislative or regulatory requirements for retention of health records, PI in electronic form will be retained in accordance with the iEHR Privacy and Security Directive on Retention and Disposal of Electronic Personal Information.

9. ACCURACY

1. Health shall undertake reasonable measures to ensure that PI is as accurate, complete and up-to-date as is necessary to eliminate or minimize the risk that inaccurate information may be used to make a decision about the client.
2. Where it is found that PI is inaccurate or incomplete, or a client successfully demonstrates that their PI is inaccurate or incomplete, Health will ensure that the PI is amended or make a note of the requested correction in the client's health record to which the information relates.
3. Information contained within client health records will not be deleted. The original information will be maintained, with any amendments or corrections made in a transparent manner.
4. Health shall notify public bodies and third parties who have received PI in the twelve months prior to a request for correction that such PI has been amended or that a note of the requested correction has been added to the client record to which the information relates.

10. SAFEGUARDS

1. Health shall ensure that appropriate physical, administrative and technical safeguards are in place to protect PI against loss, theft, and unauthorized access, use, disclosure, copying, or modification.

11. OPENNESS

1. Health shall provide a written public notice to clients and the public that:
    a. Provides a general description of Health's information handling practices;
    b. Describes how to contact the person accountable and responsible for the protection of PI collected, used, disclosed, stored and retained in relation to eHealth systems;
    c. Describes how a client may obtain access to, or request correction of a record of PI;
    d. Describes how a client may make a complaint regarding the handling of their PI; and
    e. Is written in plain language and respects the language laws of Nunavut.
2. Such a public statement shall be posted at all facilities where Health collects PI, in a location clearly visible to clients.

12. INDIVIDUAL ACCESS

1. Clients will be given supervised access to their PI or a copy of their PI upon providing a signed release form or if an alternative method of request was accepted and documented[1], unless Health has made a determination that access to such PI could reasonably be expected to result in immediate and grave danger to the individual's mental or physical health or safety.
2. Upon receiving a request, Health shall provide to clients an account of all third parties to whom their PI has been disclosed to. When it is not possible to provide a list of the third parties to which PI about a client has been disclosed to, Health shall provide a list of third parties to whom it may have disclosed their PI to.
3. Health shall provide a timely response to a client's request for access to their PI and to any request for correction or amendment, as required under applicable legislation.
4. Health may charge a fee for individuals to obtain copies of their PI in accordance with applicable legislation.

13. CHALLENGING COMPLIANCE

1. Health will put in place procedures to receive and respond to complaints and inquiries about its policies, directives and practices relating to the handling of PI in association with all eHealth systems.
2. Health will make reasonable effort to investigate all complaints. If a complaint is found to be justified, Health will take appropriate measures to resolve the complaint and reduce the risk of a future occurrence.

14. INFORMATION PRIVACY PROGRAM

1. The Information Privacy Program shall include:
    a. Measures to ensure compliance with ATIPP and any other applicable legislation in relation to the collection, use, disclosure, and protection of PI;
    b. Privacy and security training for employees and contractors of the GN;
    c. A process to receive, investigate and resolve questions or complaints;
    d. A program to monitor and audit access to records of PI in the iEHR and other eHealth systems to detect privacy and security breaches and ensure compliance with ATIPP, other applicable legislation, and Health's iEHR Privacy and Security Directives ;
    e. A process for responding to potential privacy breaches in accordance with ATIPP, including notification to the Information and Privacy Commissioner and/or clients as applicable;
    f. Investigation of privacy breaches and recommendations for corrective action to senior management;
    g. Conducting, or overseeing the development of Privacy Impact Assessments for components of the GN eHealth systems and infrastructure;
    h. Communications material for the public;
    i. Providing guidance to departmental managers who are developing agreements or contracts with third parties who require access to PI; and
    j. Providing guidance to health care personnel and departmental managers on the management of requests for access to, and correction of, health records by clients in both paper and electronic formats.

[1] A client may make an oral request for access where the individual's ability to read or write in an Official Language is limited or the individual has a physical disability or condition that impairs the individual's ability to make a written request.

15. VIOLATIONS

1. Any violation of this eHealth Information Privacy Directive, or any related topic-specific directives, standards and operating procedures by an employee of the GN is subject to the disciplinary policies and procedures of the GN.
2. Any violations of this eHealth Information Privacy Directive, or any related topic-specific directives, standards and operating procedures by a supplier, vendor or contractor or their respective employees and agents, is subject to remedies identified in the respective agreement or contract. Health may request the removal of a supplier, vendor, contractor or their respective employees and agents upon the occurrence of any such violation.

16. ADMINISTRATION OF THIS DIRECTIVE

This directive will be reviewed on an annual basis by the Deputy Minister of Health or immediately upon the occurrence of any privacy breach investigation of an authorized collection, use or disclosure of PI or a negative finding in a Privacy Impact Assessment or audit. Topic-specific directives will also be reviewed upon the occurrence of a privacy breach as applicable given the nature of the breach. A report of such review will be provided to the Minister of Health.

17. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE		
	iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
Password Management for eHealth Systems Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			3
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) on matters concerning the management of passwords for eHealth Systems, including the interoperable Electronic Health Record (iEHR) system.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Section 42 of ATIPP requires Health to protect personal information (PI) "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

2. PRINCIPLES

1. Health shall manage and control passwords to enable access to eHealth Systems in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to protect PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
    d. Each employee and contractor of the GN who is granted access to eHealth Systems and/or associated system assets is accountable and responsible for the protection and use of their password(s).
    e. Each employee and contractor of the GN who is granted access to eHealth Systems and/or associated system assets will take reasonable measures to protect their password(s) in accordance with this directive.

f. All user activity, including access to eHealth Systems, is subject to monitoring and audit by the GN.

3. SCOPE AND APPLICABILITY

This Password Management for eHealth Systems Directive applies to:

1. All employees, contractors, agents of the GN, and all vendors and suppliers of products and services to the GN, who access, use, operate and/or support eHealth systems.
2. All eHealth and associated system assets including:
    a. Sensitive data that includes:
        i. PI;
        ii. System audit logs; and
        iii. System and security administration data (e.g. technical security configurations, authentication and password data);
    b. Hardware, including mobile devices and tele-networking equipment;
    c. Software; and
    d. Network and communications resources.

4. PASSWORD MANAGEMENT

1. Users of eHealth Systems are required to keep personal passwords confidential and to keep group passwords solely within the members of the group.
2. Users should be aware that the deliberate sharing or distribution of personal passwords is considered a security breach and will be investigated and reported by the appropriate authorities.
3. Users will be assigned a secure temporary password, which must be changed immediately upon signing into the system for the first time, or the first time after a password has been replaced or reset.
4. The identity of users will be verified prior to providing a new, replacement or temporary password.
5. Temporary passwords will be given to users in a secure manner.
6. Temporary passwords should be unique to the user and should not be guessable.
7. Passwords will not be stored on a computer system in an unprotected form.
8. Default vendor passwords will be altered following installation of systems or software.
9. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these should be changed immediately upon termination or change of employment, contract or agreement (e.g. group account).
10. The maximum life for any password will be no more than 90 days, after which the password must be changed. Systems will be configured to force a password change after 90 days or a lesser time period defined by the Director of Health Information Technology.
11. No previously used password can be re-used until after at least 24 consecutive changes
12. Every new password must contain the following:
    a. A minimum of eight characters;
    b. English uppercase (A through Z);
    c. English lowercase (a through z);
    d. Numerals (0 through 9);
    e. Non-alphanumeric (such as !, $, #, %).
13. The password cannot contain the account name, the full name, or three or more consecutive characters from the username.
14. All passwords will be case sensitive.

5. ADMINISTRATION OF THIS DIRECTIVE

1. This directive will be reviewed on an annual basis by the Deputy Minister of Community and Government Services (CGS) and Deputy Minister of Health or immediately upon commencement of any security breach investigation related to password management or a negative password control finding in a Threat and Risk Assessment or security audit. A report of such review will be provided to the Minister of CGS and the Minister of Health.

6. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

_____ _____

Deputy Minister
Department of Community and Government Services

Date

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE		
	iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
Collection, Use and Disclosure of Personal information in eHealth Systems Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			6
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) regarding the collection, use and disclosure of personal information (PI) in eHealth Systems, including the interoperable Electronic Health Record (iEHR) system.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP); legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

2. PRINCIPLES

1. Health shall collect, use and disclose PI in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to protect PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
    d. Every individual has a basic need for privacy and a legal right to have control over the collection, use and disclosure of their PI.
    e. PI shall be collected, used and disclosed only by authorized individuals in accordance with ATIPP, other applicable legislation, and Health's policies and directives respecting the privacy and security of PI.

3. SCOPE AND APPLICABILITY

1. This Directive applies to:
    a. All employees, contractors, and agents of the GN who access, use, operate and/or support eHealth systems.

b. All PI collected, used, disclosed, and retained by the GN in association with eHealth systems.

4. COLLECTION OF PERSONAL INFORMATION

1. PI shall only be collected for the purposes permitted under ATIPP or other applicable legislation.
2. Clients shall be notified about the purposes for the collection of PI at or before the time of collection through the use of a written public notice.
3. Health, in consultation with the Department of Justice, will investigate all requests to collect PI where such collection is not authorized by legislation. If the Deputy Minister has authorized the request to collect such PI, then a process will be developed for obtaining the express consent of the client prior to the collection of his/her PI in accordance with applicable legislation.

5. USE OF PERSONAL INFORMATION

1. Health uses PI stored in eHealth systems for the purpose of providing health services and programs encompassing the following broad categories: acute care, primary care, public health, population health, prevention services, and mental health services and for the overall planning and management of the health care system.
2. PI may be accessed by health care providers within the client's circle of care, provided that the client is currently under the care of the health care provider(s) requesting the information, and the information being released relates directly to the health care provider(s) field of work.
    a. "Circle of care" means physicians, nurses, allied health professionals, and specialists presently providing care to the client.
3. PI shall not be used for any other purpose unless permitted by ATIPP or other applicable legislation.
4. Health will investigate all requests to use PI for a purpose that is not authorized by legislation. If the Deputy Minister of Health authorizes a request to use PI for a new purpose, then a process will be developed for obtaining the express consent of the client prior to the use of their PI.

6. DISCLOSURE OF PERSONAL INFORMATION

1. PI shall only be disclosed through a secure and authorized process approved by the Deputy Minister of Health.
2. Health must document all disclosures in the applicable client file, including a detailed summary of what was disclosed; for what purpose it was disclosed; to whom it was disclosed; and whom it was disclosed by.
3. Health must ensure that the identity of the individual to whom the PI is to be disclosed to has been confirmed. It is not acceptable to rely on past confirmations of identity.[1]
4. All disclosures of PI not listed under Permitted Disclosures (see below) require the express consent of the client before the release of their PI, including but not limited to: relatives and friends of the client; an employer; insurance companies; and lawyers[2].
5. All Permitted Disclosures will require some form of written authorization except for disclosures within the client's circle of care, to notify the next of kin, to provide access to Health Insured Services, or to the Registrar of Disease Registries. The written

[1] See ATIPP Regulation R-206-96 section 5(4) for proofs of identify for persons requesting or consenting to disclosure of PI.
[2] Except for lawyers within the Department of Justice as provided for under ATIPP section 48(c) and (l).

authorization must state the legislative authority that the requestor is relying on to collect the PI and the purpose to which the information is required.

6. All disclosures of PI must be limited to that which is reasonably necessary for the authorized purpose.
7. Permitted Disclosures - The table below summarizes disclosures permitted by ATIPP and other applicable legislation without the client's express consent. PERMITTED DISCLOSURES MUST STILL COMPLY WITH THE AFOREMENTIONED REQUIREMENTS, INCLUDING LIMITING DISCLOSURE TO THAT WHICH IS NECESSARY FOR THE AUTHORIZED PURPOSE, DOCUMENTING THE DISCLOSURE AND DISCLOSING INFORMATION IN A SECURE MANNER.

REQUESTER	PERMITTED DISCLOSURES[3]	LEGISLATIVE AUTHORITY
Board of Inquiry under the Medical Profession Act	PI may be disclosed to the Board of Inquiry upon proper notice to a witness stating the documents the witness is required to produce.[4]	Medical Profession Act s. 31(1) & (2)
Client	A client can request to see their own PI according to the ATIPP Act (with some restrictions). The Deputy Minister may disclose information relating to the mental or physical health of an individual to a medical or other expert for an opinion as to whether disclosure of the information could reasonably be expected to result in immediate and grave danger to the client's mental or physical health or safety.	ATIPP s.5 ATIPP Regulations s.4
Coroner	Upon receipt of a Warrant issued by the Coroner to take possession of a body, Health may disclose PI to the Coroner to assist in the investigation of a reportable death.	Coroner's Act s.9. (1)
Guardian/Child Protection Worker	Health may disclose PI to a client's court appointed guardian upon proof of a guardianship order noting the guardian's specific rights to the disclosure of the PI and the period to which the guardianship applies.	Guardianship and Trusteeship Act s.11(2)

[3] Note legislative authorities to disclose personal information have been qualified in this table to relate to the disclosures of personal health information relevant in a health care setting; the actual legislative authority may permit a broader disclosure of personal information not relevant to the health care setting.
[4] The Medical Profession Act does not authorize the disclosure of PI without the individual's consent except during the course of an inquiry under section 31(1) & (2).

REQUESTER	PERMITTED DISCLOSURES[3]	LEGISLATIVE AUTHORITY
	PI may be disclosed to a Child Protection Worker where the client is under the temporary or permanent custody of the Director of Child and Family Services. An order granting permanent or temporary custody of the client must be provided.	Hospital Standards Regulations s.74(1)(g)
	In circumstances where a client has been apprehended and no order exists, PI may be disclosed to a Child Protection Worker only to the extent required for purposes of the current care and treatment of the client.	Child and Family Services Act s.35
Health Insured Services	Health may disclose PI to Health Insured Services to support administrative and billing purposes.	ATIPP s.48(a)
Healthcare providers outside of the GN within the circle of care	Health may disclose PI to healthcare providers and healthcare facilities out–of-territory, but within the circle of care, for the provision of care.	ATIPP s.48(a)
Information & Privacy Commissioner of Nunavut	Health may disclose PI to the Information & Privacy Commissioner where the information is necessary for the performance of the Commissioner's duties.	ATIPP s.48(i)
Medical Health Officer	Upon written request, Health may disclose PI to the Medical Health Officer.	Hospital Standards Regulations s.74(1)(b)
Next of Kin	PI may be disclosed to notify the next of kin of an injured, ill, or deceased individual but Health may not disclose the nature of the injury or illness.	ATIPP s.48(r)
Registrar of Disease Registries	Health may disclose PI, in a form approved by the Registrar, where a health care professional who examines, diagnoses or treats a person in respect of a reportable disease or performs or causes to be performed a reportable test on a person. Such form must limit the information provided to that which is authorized by the Disease Registries Act.	Disease Registries Act s.3 & s.5
Researcher	PI may be disclosed for research purposes when authorized under ATIPP and approved by the GN's Research Committee and the Deputy Minister of Health, provided that such disclosure is in compliance with the related ATIPP requirements.	ATIPP s49(d) and Regulations R-206-96 s.8

REQUESTER	PERMITTED DISCLOSURES[3]	LEGISLATIVE AUTHORITY
Substitute Consent Giver	A substitute consent giver is entitled to receive all information concerning the client and the proposed treatment that is necessary for an informed consent. Where a client is mentally incompetent, the substitute consent giver is entitled to examine and copy the client's health record. Where a client is mentally competent, a person who acted as a substitute consent giver at a time when the client was mentally incompetent is entitled to examine and copy that portion of the client's health record that pertains to decisions made by the person in the capacity of substitute consent giver.	Mental Health Act s.19.4 and s. 49.4
Under Subpoena, Warrant, or Order	Requests for PI by a court of law in the form of a subpoena, warrant or order of the court authorizing disclosure of specific information. Disclosure of information must be limited to that which is provided for in the warrant, subpoena, or order.	ATIPP s.48(n)
Veteran Affairs	Upon written request from Veteran Affairs, Health may disclose PI to the Department of Veterans Affairs (Canada) with respect to a client who is a member or former member of the army, naval or air force of Canada, or who is otherwise eligible to receive services from that department.	Hospital Standards Regulations s.74(i)
Vital Statistics	PI required for reporting births, stillbirths or deaths may be disclosed to the Registrar General.	Vital Statistics Act s.2, 12 & 19
Workers' Safety and Compensation Commission	Upon receipt of a completed form letter from the Workers' Compensation Commission, Health may disclose any PI that is necessary for the Workers' Safety and Compensation Commission to determine a claim for compensation. A health care provider who examines or treats a worker under the Workers' Compensation Act is authorized to submit a report to the Commission, when such report may contain PI.	Workers' Compensation Act s.30 Hospital Standards Regulations s.74(1)(h) Workers' Compensation Act s.25(1)

REQUESTER	PERMITTED DISCLOSURES[3]	LEGISLATIVE AUTHORITY
Other	PI may be disclosed where such disclosure is authorized under a law of Nunavut or Canada.[5]	
	PI may be disclosed when the disclosure is necessary to protect the mental or physical health or safety of any individual.	ATIPP s.48(q)
	PI may be disclosed when the disclosure is in the public interest or would clearly benefit the individual to whom the PI relates as authorized by the Deputy Minister.	ATIPP s.48(s)
	PI may be disclosed to carry out a formal examination of a governmental program wherein such examination is sanctioned by statute, regulation or public policy.	Regulations R-206-96 s.6
	PI May be disclosed for audit purposes to the Auditor General or Department of Finance.	ATIPP s.48(j) Regulations R-206-96 s.7

8. ADMINISTRATION OF THIS DIRECTIVE

This directive will be reviewed on an annual basis by the Deputy Minister of Health or immediately upon the occurrence of any privacy breach investigation of an authorized collection, use or disclosure of PI or a negative finding in a Privacy Impact Assessment or audit. A report of such review will be provided to the Minister of Health.

9. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

[5] Such as audit and investigation powers provided under various Nunavut legislation – e.g. The Midwifery Profession Act Section 26 (practice auditors) & Section 34 (investigations).

Department of Health Government of Nunavut	DEPARTMENT OF HEALTH DIRECTIVE		
	iEHR PRIVACY AND SECURITY DIRECTIVE		
TITLE:		**SECTION:**	**POLICY NUMBER:**
eHealth Access Control Directive			
EFFECTIVE DATE:	**REVIEW DUE:**	**REPLACES NUMBER:**	**NUMBER OF PAGES:**
			4
APPLIES TO:			
All employees, contractors, and agents of the GN who use eHealth systems			

1. PREAMBLE

The purpose of this directive is to provide guidance to employees, contractors, and agents of the Government of Nunavut (GN) on matters concerning the management of access to eHealth Systems, including the interoperable Electronic Health Record (iEHR) system.

The Department of Health (Health) is subject to the *Access to Information and Protection of Privacy Act* (ATIPP), legislation that has been established to make public bodies more accountable to the public when it comes to information handling and the protection of privacy. Personal information as defined by ATIPP includes personal health information (PHI).

Section 42 of ATIPP requires Health to protect personal information (PI) "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

Clients expect and trust that Health will protect the confidentiality, privacy and integrity of their PI. Meeting these expectations is essential to promoting client safety and retaining client trust and loyalty.

2. PRINCIPLES

1. Health shall control access to eHealth systems in conformance with the following principles:
    a. The priority of strengthening the public service by advancing eHealth Infrastructure, which provides improved, efficient, and effective management of PI.
    b. The Inuit Qaujimajatuqangit principles of Piliriqatigiinniq (working together for a common cause), Inuuqatigiitsiarniq (respecting others, relationships and caring for people), Tunnganarniq (fostering good spirit by being open, welcoming and inclusive), and Pilimmaksarniq (development of skills through practice, effort, and action).
    c. The GN, which includes Health, has a statutory obligation to protect PI by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.
    d. Role-based access control will be employed to enable access to eHealth systems.
    e. Role definitions for users will be defined by Health in consultation with stakeholders.
    f. Users of eHealth systems will be assigned roles by their managers.
    g. Access to eHealth systems and system resources will be granted on a need-to-know basis, based on the user's role.

h. All user activity, including access to eHealth systems, will be subject to monitoring and audit by the GN.

3. SCOPE AND APPLICABILITY

This eHealth Access Control Directive applies to:

1. All users including employees, contractors, and agents of the GN, and all vendors and suppliers of products and services to the GN, who access, use, operate and/or support eHealth systems.
2. Both physical and logical access to eHealth systems and associated system assets.
3. All eHealth and associated system assets including:
    a. Sensitive data that includes:
        i. PI;
        ii. System audit logs; and
        iii. System and security administration data (e.g. technical security configurations, authentication and password data);
    b. Hardware, including mobile devices and tele-networking equipment;
    c. Software; and
    d. Network and communications resources.

4. ROLES AND RESPONSIBLITIES

1. Health has primary responsibility for determining the sensitivity of eHealth system assets, including PI. PI that is processed or stored in eHealth systems will be classified as confidential.
2. The Department of Community and Government Services (CGS) maintains the responsibility for controlling access to technical environments and infrastructure containing eHealth systems.
3. Access control measures will be implemented commensurate with the sensitivity of the asset and the threat of compromise as determined by any Threat and Risk Assessment (TRA).

5. DEFINING ACCESS PRIVILEGES

1. Access to system assets will be restricted based on role, job, function and work group on a strict need-to-know basis.
2. The Health Information Division (HID) will develop an access control matrix defining user roles and access privileges. Roles and corresponding access privileges will be developed in consultation with user departments and user groups.
3. The HID may define work groups and enable access to PI and other eHealth assets to individual users based on the work group.
4. The HID may enable functionality in an eHealth system that associates users with the records of their clients. This can allow the user to grant discretionary access rights to another registered user.

6. ASSIGNMENT OF ACCESS PRIVILEGES

1. The manager or supervisor of the user to whom access will be granted will determine assignment to a role or group with corresponding access privileges. A single user may have multiple roles.
2. The manager or supervisor of the user to whom access will be granted must confirm that the user has received the required training, signed a confidentiality agreement, and has read and understood: the GN's Privacy Breach and Incident Policy; the Acceptable E-Mail and Internet Usage Policy; and Health's iEHR Privacy and Security Directives.

7. USER IDENTIFICATION AND REGISTRATION

1. The HID will establish user registration procedures that will ensure:
    a. The required level of user identification that is provided is consistent with the assurance required given the sensitivity of the PI and system assets, and the functions that will become available to the user;
    b. Each potential user has a legitimate relationship with the organization; and
    c. Each potential user has a legitimate need to access PI and other sensitive system assets.
2. Authorized users will be assigned a user ID that in combination with other identifiers (e.g. passwords, security tokens, and facility or location identifiers) can uniquely identify the user.
3. The HID will enable reporting functionality in eHealth systems to report, for a given user:
    a. Which records the user can access;
    b. Which portions of the record the user can access; and
    c. Which privileges (i.e. view, add, delete, modify) the user possesses with respect to each of these records.
4. Access privileges for each user will be reviewed and renewed on an annual basis, at which time user registration details will be reviewed and updated, as required.
5. Access privileges for users will be immediately revoked where such access is no longer required, such as on termination of employment or change in job function or role. The HID will develop procedures for the revocation of access privileges for eHealth systems.
6. There will be clear separation of duties between system administration personnel who grant access to sensitive data and resources, users, user's supervisors, and managers who access and use system assets. Systems administrators will not be able to grant themselves access to eHealth resources, including PI.

8. AUDIT LOGGING AND MONITORING SYSTEM ACCESS

1. The HID will enable audit logging and reporting functionality in the eHealth systems in order to record in an audit log every instance of a user viewing, adding, modifying, deleting or archiving PI.
2. The HID will enable audit logging and reporting functionality in the eHealth system to report every access to a client's PI.
3. The HID will secure access to audit logs and audit tools to prevent misuse or compromise.
4. The HID will implement a monitoring and audit program to determine if there are unauthorized accesses to eHealth system assets, including PI, and taking appropriate action when a security or privacy breach is suspected.

9. USER ACCESS TO eHEALTH SYSTEMS

1. Each user will only access the eHealth system and services in a single role (i.e. users who have been registered with more than one non-overlapping role must designate a single role during each eHealth system session).
2. Where required, authentication may include digital certificates, secure tokens or biometrics to access sensitive system assets.
3. Physical and logical access to unattended workstations will be restricted and measures implemented to ensure that an unauthorized person will not be able to use a workstation while the eHealth system is active.

10. CONTROLLING ACCESS TO TECHNICAL ENVIRONMENTS

1. The Department of Community and Government Services (CGS) will ensure that all connections to remote services and applications are authenticated, including connections via the Internet.
2. CGS will control access to eHealth network diagnostics and network management services, including access to diagnostic ports and services on networks hosting those components.
3. CGS will control access to and restrict the use of eHealth system utility programs.

11. ADMINISTRATION OF THIS DIRECTIVE

This directive will be reviewed on an annual basis by the Deputy Minister of CGS and the Deputy Minister of Health, or immediately upon commencement of any security breach investigation related to access control or a negative access control finding in a TRA or security audit. A report of such review will be provided to the Minister of CGS and the Minister of Health.

12. AUTHORIZATION

_____ _____

Deputy Minister
Department of Health

Date

_____ _____

Deputy Minister
Department of Community and Government Services

Date