



IDENTIFICATION

Department		Position Title	
Health and Social Services		Chief Health Privacy Officer	
Position Number(s)		Community	Division/Region(s)
49-14583		Yellowknife	Information Services

PURPOSE OF THE POSITION

The Chief Health Privacy Officer is responsible for the development and implementation of a Health Privacy Framework for the Northwest Territories (NWT) and the promotion of a culture of health privacy within the NWT health and social services system. The Chief Health Privacy Officer oversees and promotes a client focused, balanced approach to the protection and sharing of information in the NWT health and social services system to enable the delivery of better patient care. The Chief Health Privacy Officer is accountable for providing leadership in the design, management and implementation of NWT health specific privacy regulatory and policy framework. This leadership requires thinking within general and highly complex privacy principles and broadly defined objectives. Policies for the work done by the incumbent are not yet set. There are no functional precedents for the work carried out by the incumbent. The incumbent receives just general direction and guidance on larger organizational objectives. The incumbent provides leadership that reaches beyond the Department of Health and Social Services (DHSS). The incumbent provides leadership across the NWT health and social services system and to private physicians, pharmacists and any other health care professionals that make up part of the Health Privacy Framework in the future. The incumbent shares responsibility and control over Territorial health information systems, such as the Electronic Medical Record and Child and Family Services Information System, to ensure privacy requirements are met by design. In addition, the Chief Health Privacy Officer leads the development and implementation of privacy initiatives within the NWT health and social services system to ensure the Health Information Act (HIA) and the Access to Information and Protection of Privacy Act (ATIPP) are considered, implemented and adhered to. The incumbent is considered the principle expert on health privacy throughout the GNWT and leads in providing the Minister of Health and Social Services with strategic analysis, guidance and advice respecting health privacy and the status of the NWT Health Privacy Framework. The incumbent has a controlling responsibility in how the NWT Health

Privacy Framework is implemented across the entire health and social services system. The incumbent is responsible for setting functional policies and frameworks that enable health care providers throughout the health and social services system to deliver services in compliance with the Health Privacy Framework.

SCOPE

Located in Yellowknife, the Chief Health Privacy Officer reports to the Chief Information Officer.

Technology and an integrated approach to the delivery of services have raised expectations and empowered people to ask for greater levels of privacy and security when it relates to the management of their personal health information. The Chief Health Privacy Officer will be responsible for leading the development, communication, delivery, monitoring, mitigation and evaluation of an NWT Health Privacy Framework. This Framework will be significantly valuable to the NWT health and social services system, and at the same time, will be entirely new to health care providers both public and private, the public, and GNWT staff. The Framework will allow for improved health system planning through evidence-based funding and program delivery; easier information flows between health care providers; coordinated and team-based services; and a culture of privacy where patients trust their providers and can participate in how their health information is managed. The Framework is fundamental to providing better care to NWT residents, one of the main priorities of the Department and GNWT. In order to establish this Framework, the incumbent is expected to have a high amount of accountability, freedom to act, and decision-making authority.

The Chief Health Privacy Officer oversees and ensures the development and implementation of health and social services policies concerning the privacy, security, collection, use, disclosure, destruction, access, management and breach of health information. The incumbent has responsibility for setting and approving health privacy procedures, core principles and objectives, standards and best practices that are to be complied with throughout the NWT health and social services system and by private NWT health care professionals.

The Chief Health Privacy Officer has decision-making authority and approves the Territorial electronic health information system auditing and monitoring programs that track and promote proper protection of patient privacy throughout the NWT. The incumbent is responsible for ensuring Health Privacy Unit staff carries out the approved auditing and monitoring programs. The incumbent is responsible for reporting to the Minister, the Deputy Minister, senior Department Management, and Health and Social Services Authorities (HSSAs) on the status of the Territorial auditing and monitoring programs.

The Chief Health Privacy Officer leads the review of Departmental privacy impact assessments (PIAs) and HSSA PIAs relating to Territorial initiatives and for new and updated communication technologies and information systems, and supports the development of Departmental and HSSA PIAs. In signing off on these PIAs, the Chief Health Privacy Officer is accountable for making the determination that the GNWT is taking on a reasonable amount of risk weighed against the value these communication technologies and information systems

will have for patient care, and that risks will be sufficiently mitigated and monitored.

The Chief Health Privacy Officer provides expertise in the area of health privacy and ensures that the strategic advice, analysis and recommendations coming out of the Health Privacy Unit are sound, feasible, reflective of health privacy best practice, and also forward looking. The Chief Health Privacy Officer is responsible for briefing the Minister, the Deputy Minister, senior Department Management, and HSSAs, on this expertise, strategic advice, analysis and recommendations. As well, the position assists in developing Ministerial and Departmental positions and approaches that reflect a very high level of political, financial and social sensitivity and responsiveness.

The incumbent is expected to liaise with the Information and Privacy Commissioner, Territorial and National health care professional organizations, federally-supported health agencies, such as Canada Health Info way and the Canadian Institute of Health Information, and internationally-recognized health privacy organizations. The Chief Health Privacy Officer coordinates a number of Interdepartmental privacy committees and represents the GNWT on inter jurisdictional health information privacy committees. In addition, given the nature of the health and social services system, there is the requirement to work with colleagues in other jurisdictions to benefit from the services available outside the NWT. The Chief Health Privacy Officer also addresses government wide and national reporting requirements working in collaboration with the Chief Information Officer, HSSAs, and other stakeholders within the system. The position liaises with senior executives in other departments, central agencies, the media, and representatives of public interest groups to discuss and keep current with respect to health privacy legislation, policies, and security trends, and to promote the NWT Health Privacy Framework.

The position is responsible for designing and coordinating the system-wide strategic and business-planning processes, including environmental scans, evaluation, outcomes and measures development, and results reporting as these pertain to the Health Privacy Framework.

The position functions at a senior level in the Department and must possess a wide mix of managerial, communications, analytical, public relations and diplomatic skills as well as a sound knowledge of current and evolving GNWT policies, programs, issues and developments. The Chief Health Privacy Officer must carry out the responsibilities of the position recognizing the complexities, Inter-relationships and diverse goals of the system.

The Chief Health Privacy Officer will face an immediate and substantial challenge with respect to leading and overseeing activities necessary to bring the HIA into force in a timely manner. Preparatory work will include overseeing the development of a complete policy and regulatory framework; overseeing the development of an HIA Manual, training tools and resource materials; ensuring staff throughout the health and social services system and private health care professionals are trained and familiar with the HIA, health privacy policies, procedures, standards, best practices, and risk management; overseeing the development and delivery of a public awareness campaign; overseeing the establishment of an NWT Research Ethics Committee; and leading the establishment of an NWT Health Information Governance

Committee. Once in force, the incumbent will coordinate the GNWT application to Industry Canada for Personal Information Protection and Electronic Documents Act (PIPEDA) substantial similarity status to allow all NWT health care professionals, private and public, to adhere to the same set of health privacy rules and regulations.

The Chief Health Privacy Officer is the main point of contact for all the Department's privacy-related requests and issues. The incumbent oversees the management of the Department's public government ATIPP and records management responsibilities. In addition, the Chief Health Privacy Officer leads the Health Privacy unit in providing strategic advice, analysis and recommendations regarding the collection, use and disclosure of information in accordance with the Adoption Act, Child and Family Services Act, Mental Health Act, Public Health Act, and Vital Statistics Act.

The incumbent is responsible for an annual budget of approximately \$500,000 and three officer level positions

- Senior Health Privacy Officer;
- Senior Privacy Specialist; and
- ATIPP and Health Privacy Officer.

RESPONSIBILITIES

1. Oversees the policy development necessary for the establishment and implementation of the Health Privacy framework.

- Is accountable for the creation of a Health Privacy Framework for the NWT health system through policy development;
- Oversees the development and Implementation of privacy and security policies, procedures, safeguard measures and best practices associated with the collection, use, disclosure, access, management and auditing of personal health information processed and stored in Departmental and territory-wide information systems, to guide employees and contractors of the DHSS and the HSSAs on matters related to health information privacy and security;
- Oversees the development of best practices and core principles and objectives for privacy and security policies, procedures and safeguard measures associated with the collection, use, disclosure, access, management and auditing of personal health information processed and stored in private health care provider electronic health information systems across the NWT, such as systems set up in private pharmacies and private physician clinics;
- Oversees the development of health privacy policies specific to de-identification standards, data matching, and data manipulation;
- Oversees the development of health privacy policies specific to research and health system planning, evaluation and management;
- Oversees the development of standards, best practices, templates, and tools for information sharing agreements, information management agreements, and research agreements to ensure compliance with the HIA;

- Leads on policy rationale development for regulations under the HIA; ensures HIA regulations reflect privacy program requirements;
- Responsible for general policy development in support of the principles of health privacy;
- Monitors compliance with approved policies;
- Monitors legislative changes and other developments, and ensures amendment to Departmental policies as required;
- Accountable for identifying and prioritizing emerging issues, overlaps or gaps in the Health Privacy Framework and addressing these, considering the overall strategic priorities of the NWT health system;
- Establishes and updates privacy breach protocols to be complied with by the DHSS, HSSAs, and private health care providers; and
- Communicates best practices and core principles and objectives to private health care providers; acts as knowledge resource for private health care providers; promotes a culture of health privacy across the NWT.

2. Responsible for the enforcement and promotion of the HIA across the NWT. Leads on ensuring the Department and the GNWT meet their responsibilities and obligations under the HIA.

- Responsible for developing the annual GNWT Response to the Standing Committee on Government Operations' review of the Information and Privacy Commissioner's annual HIA report;
- Responsible for ensuring the GNWT Response is submitted in a timely fashion and is congruent to overarching GNWT priorities and positions while also reflective of the current and future state of the NWT health and social services system;
- Ensures the Department fulfills a leadership role in ensuring the NWT health and social services system and private health care professionals comply with the HIA;
- Provides leadership in the promotion of the HIA across the NWT;
- Ensures Departmental compliance in regards to information management arrangements;
- Ensures the Department has designated contact persons, as required under the HIA;
- Establishes and ensures the implementation of a standard process for receiving, evaluating and responding to requests for access to personal information and/or personal health information held by the Department, including for research, law enforcement, and health systems planning;
- Ensures the coordination of all HIA access requests received by the Department; and
- Ensures Health Privacy Unit staff provide advice to the other HIA access request coordinators and designated contact persons in the NWT, both private and public, to promote compliance with the HIA.

3. Ensures the development and delivery of training materials, risk management tools, resource materials, and training modules for NWT health and social services system decision-makers, staff, and health care providers, and private health care professionals. Ensures the development and delivery of a public awareness campaign for NWT residents.

- Oversees the development and ongoing updating of an HIA Manual, form and template documents, and online workshops and tools;
- Oversees the development and delivery of HIA training programs, online tutorials, and workshops to employees and contractors of DHSS, HSSAs, and private health care professionals across the NWT on information privacy and security policies, procedures, safeguard measures, best practices, and core principles and objectives to ensure compliance with the HIA;
- Identifies a need for and oversees the provision of general privacy training to health and social services system decision-makers, staff, and health care providers;
- Leads the development and delivery of a large-scale public awareness campaign to notify the public on the Health Privacy Framework and their rights under the HIA;
- Ensures the Information and Privacy Commissioner and Members of the Legislative Assembly are made aware of and updated on the public awareness campaign;
- Ensures ongoing information is shared with staff and practitioners on the obligations under ATIPP, HIA and privacy practices;
- Oversees the ongoing development of appropriate information for the public about the Department's privacy practices; and
- Oversees the ongoing development of public information on the HIA and application, as well as on ATIPP.

4. Responsible for leading additional HIA implementation activities.

- Oversees the establishment of an NWT Research Ethics Committee, required under the HIA to review all NWT-based research applications requiring access to personal health information;
- Ensures support is provided to the NWT Research Ethics Committee in order to ensure its functionality;
- Spearheads the establishment of an NWT Health Information Governance Committee for the NWT health and social services system; and
- Coordinates the GNWT application to Industry Canada for Personal Information Protection and Electronic Documents Act (PIPEDA) substantial similarity status to allow all NWT health care professionals, private and public, to adhere to the same set of health privacy rules and regulations.

5. Oversees the development and implementation of the Auditing and Access Controls Privacy Program

- Ensures the establishment, evaluation, implementation, and expansion of auditing programs for Departmental and Territory-wide electronic health information systems, including approving changes, establishing audit plans and ensuring the organization of DHSS and HSSA staff to deliver auditing programs;
- Accountable for the identification and prioritization of emerging issues, overlaps or gaps in the Health Privacy Program and is accountable for effecting change and ensuring the implementation of solutions, considering the overall strategic priorities of the NWT health system;
- Ensures direction is provided to project managers, system developers and business analysts concerning privacy and security requirements, the integration of "Privacy by

Design" principles into the systems development lifecycle, and the testing of privacy functionality and business processes in Departmental and territory-wide electronic health information systems;

- Ensures audits of access to personal health information are carried out on the iEHR, EMR, and additional Departmental and Territory-wide electronic health information systems to detect privacy breaches; accountable for initiating action to investigate and resolve breaches;
- Provides guidance to the Deputy Minister, Department senior management, and HSSA executive and senior managers who are developing agreements or contracts with third parties who require access to electronic PHI including contractors, researchers, other territorial or provincial jurisdictions, or health service providers to ensure that privacy and confidentiality requirements are adequately addressed in contract terms and conditions;
- Establishes criteria and processes for the implementation of role based access control (RBAC) for all Departmental and Territory-wide electronic health information systems; reviews and rejects or approves requests that are an exception to the established RBAC framework;
- Ensures and oversees investigations into privacy breaches and complaints associated with DHSS and territory-wide health information systems, and ensures corrective action is taken by staff or, depending upon the severity of the breach, by senior management, including the Deputy Minister and HSSA executive management;
- Accountable for advice provided to private health care providers on privacy breaches; tracks privacy breaches originating in private electronic health information systems, where the breach affects care provided to patients in the public NWT health system;
- Accountable for ensuring patients and the NWT Information and Privacy Commissioner are notified of a privacy breach to ensure compliance with the HIA and promote a culture of health privacy in the NWT health system;
- Ensures the development and implementation of a standard process for tracking and assessing privacy incidents, and investigating where necessary;
- Endorses the development and implementation of standard processes for responding to patient/public complaints and inquiries that include working with Departmental and other organization's staff to investigate and respond as appropriate; and
- Accountable for ensuring the monitoring of all privacy and security breaches and complaints from the public associated with DHSS and territory-wide health information systems to identify trends, to detect systemic issues that may be root-causes for privacy and security incidents, and to produce updates and changes to privacy and security policies, procedures and safeguard measures and privacy breach protocols.

6. Responsible for carrying out risk management functions related to privacy impact assessments.

- Accountable for the development and review of Privacy Impact Assessments (PIAs), required under the HIA for communications technologies and information systems;
- Oversees the development and updating of PIAs for DHSS and territory-wide information systems including the iEHR, PACS, LIS, EMR and telemedicine;

- Ensures the identification of privacy and security risks, and the identification and implementation of mitigation strategies to manage identified risks;
- Procures and manages contracted expert resources in the development and updating of PIAs;
- Accountable for Departmental review of PIAs conducted by HSSAs;
- Accountable for the provision of advice to private health care professionals on PIAs to ensure best practices and compliance with the HIA;
- Responsible for ensuring the provision of and provides support on threat risk assessments for Departmental and Territory-wide communications technologies and information systems; and
- Accountable to evaluate the PIA process and past PIAs to effect change for improvement and PIA policy expansion.

7. Represents the Department on intergovernmental and interdepartmental committees and associations.

- Represents the Department at Federal/Provincial/ Territorial meetings;
- Participates in the development of nation-wide messaging and awareness campaigns;
- Leads interdepartmental working groups and committees;
- Presents Departmental and GNWT positions; and
- Makes recommendations on intergovernmental committees that reflect the Department's/GNWT's position.

8. Leads the coordination of the Department's roles and responsibilities under ATIPP and the management of the Department's government administrative records.

- Supervises the processing of the request from receipt to disclosure of records, remaining current as to status and deadlines;
- Ensures the analysis and evaluation of the implications and advisability of possible options for dealing with ATIPP requests, advising Senior Management including the Deputy Minister of these options and recommending a course of action;
- Ensures the analysis and evaluation of the sensitivity of ATIPP requests, alerting appropriate senior staff and ensuring Health Privacy staff work with them to develop and implement necessary communication strategies;
- Accountable for the evaluation, review, and revision of contracts, protocol agreements, and information sharing agreements drafted by divisions within the Department to ensure compliance with ATIPP; and
- Ensures the management of a records management system that is consistent with GNWT legislation and policies.

9. Communications

- Provides expert advice to the Minister, Deputy Minister, HSSA Executive Management, HSSA Quality Risk Managers, Senior Department Management, and private health care professionals with respect to health privacy;
- Liaises with Department staff, HSSAs, the Office of the Information and Privacy Commissioner and private health care professionals across the NWT to promote a

culture of health privacy in the delivery and management of health services in the NWT; and

- Ensures that senior officials are informed as required of key activities and risks.

10. Leads research and analysis in both the health and social domains to inform decision making and assist in business and strategic planning.

- Evaluates decision papers, policy proposals, FMB submissions and ministerial briefing materials; and
- Directs the development of briefing material, support documentation, agendas and program/policy issue summaries for use by the Deputy Minister in meetings, committees and seminars chaired or attended by the DM.

11. Manages the human and financial resources of the Health Privacy Unit.

- Manages the unit's budget;
- Ensures unit staff have access to necessary resources, supplies, equipment and information;
- Inform staff about governmental, departmental and divisional priorities;
- Develop and implement annual work plans which establish short and long term objectives for the unit;
- Organize staff, contracts, intergovernmental committees, information resources;
- Complete human resource functions within the division including staffing and performance reviews, discipline; and
- Identify training requirements and opportunities for staff.

WORKING CONDITIONS

Physical Demands

Position requires regular travel to NWT communities, including travel in small airplanes.

Environmental Conditions

Except when travelling, normal office environment.

Sensory Demands

Normal office environment.

Mental Demands

Position requires frequently dealing with individuals who hold strong views which may be inconsistent with GNWT and HSS overall direction. Must be able to cope with conflict and animated discussion of issues.

Must manage very tight deadlines, competing priorities and complex issues that can be very stressful.

Must manage the establishment of new program and regulatory framework this is particularly demanding and stressful.

Must lead meetings and actively participate in community and regional consultations on health and social services privacy framework. These events can be stressful with a great deal of emotion.

KNOWLEDGE, SKILLS AND ABILITIES

- Expert knowledge in the field of health privacy, requiring a command of diverse practices and precedents and highly sophisticated and complex concepts and principles.
- Expert knowledge of policy development, communication planning and health privacy environment.
- Expert ability to analyze, interpret and evaluate privacy and security information and apply it within the unique health and social services environment of the NWT.
- Seasoned knowledge of project management and the ability to lead large and complex privacy projects from development to implementation.
- Leadership skills to drive projects forward, effect change and encourage others.
- An ability to build and maintain excellent working relationships with colleagues throughout the NWT health and social services system, and with partners outside of government.
- Expert ability to motivate colleagues to achieve difficult goals.
- Ability to expertly represent the Department and its position accurately and professionally in a variety of consultations, meetings, presentations and other situations.
- A seasoned ability to analyze, evaluate and interpret privacy and security legislation and regulations and apply it within the unique social, economic and political environments of the NWT.
- A thorough knowledge of and ability to apply generally accepted approaches to privacy, including an ability to adapt to evolving governance structures.
- Highly effective oral and written communication skills, including presentations, briefing notes, charts and graphs, reports and publications for a wide variety of audiences.
- High level of organizational skills to manage projects, timetables and implementations.
- Advanced interpersonal skills to coordinate privacy activities to positively communicate and work with professionals at all levels of the organization as well as the public.

Typically, the above qualifications would be attained by:

This knowledge, skill and ability is normally acquired through:

- The completion of a master degree in Public Administration, Law or Business Administration;
- Six (6) years progressively more responsible experience in the development of policy and management of privacy information, including:

- Three (3) years of supervisory/management experience.
- A minimum of three (3) years progressive program development and quality improvement experience as well as experience in chairing and participating in interdisciplinary work groups.
- Skill and experience in program development and project management, plus methods of improvement, theories of change, and current concepts of team-building.
- Considerable knowledge of privacy legislation at the territorial, provincial, federal and private levels.
- Certification in information privacy an asset.

ADDITIONAL REQUIREMENTS

Position Security (check one)

- ☐ No criminal records check required
- ☐ Position of Trust – criminal records check required
- ☒ Highly sensitive position – requires verification of identity and a criminal records check

French language (check one if applicable)

- ☐ French required (must identify required level below)
 - Level required for this Designated Position is:
 - ORAL EXPRESSION AND COMPREHENSION
 - Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
 - READING COMPREHENSION:
 - Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
 - WRITING SKILLS:
 - Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
- ☐ French preferred

Aboriginal language: To choose a language, click here.

- ☐ Required
- ☐ Preferred