TD 484-20(1) TABLED ON MARCH 4, 2026

Government of | Gouvernement des
Northwest Territories
Territoires du Nord-Ouest

NWT Department of
Health and Social Services

TEN-YEAR REPORT
ON THE NORTHWEST TERRITORIES *HEALTH INFORMATION ACT*

RAPPORT DÉCENNAL SUR LA
LOI SUR LES RENSEIGNEMENTS SUR LA SANTÉ DES TERRITOIRES DU NORD-OUEST

Ministère de la Santé et
des Services sociaux des TNO

OCTOBER 1, 2025 / 1er OCTOBRE 2025

K’áhshó got’ı̨ne xədə k’é hederı ɔedı̨htl’é yerınıwę nı́ dé dúle.
Dene kədé

ʔerıhtł’ís Dëne Sųłıné yatı t’a huts’elkër xa beyáyatı theɔą ɔat’e, nuwe ts’ën yółtı.
Dëne sųłıné

Edı gondı dehgáh got’ı̨e zhatıé k’ę́é edatł’éh enahddhę nıde naxets’é edahłí.
Dene zhatıé

Jii gwandak izhii ginjìk vat’atr’ijąhch’uu zhit yinohthan jì’, diits’àt ginohkhìi.
Dinjii zhu’ ginjik

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

ᑕᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᓕᒍᐹᕆᑦ ᐃᓄᒃᑎᑐᓪᓗᕆᒪᓕᒃ, ᐅᐸᑦᑎᓂᓄᑦ ᐅᖃᓕᔨᓂᖅᑐᖅᑐᑦ.
Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.
Inuinnaqtun

kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
nēhiyawēwin

Tłı̨chǫ yatı k’ę̀è. Dı wegodı newǫ dè, gots’o gonede.
Tłı̨chǫ

Langues autochtones
request_Indigenous_languages@gov.nt.ca


10 YEAR

Table of Contents

Table of Contents

Acronyms

AI	Artificial Intelligence
ATIPPA	*Access to Information and Protection of Privacy Act*
DHSS	Department of Health and Social Services
EMR	Electronic Medical Record
GNWT	Government of the Northwest Territories
HIA	*Health Information Act*
HSS	Health and Social Services System
HSS PAC	Territorial HSS Privacy Advisory Committee
HSSAs	Health and Social Services Authorities
IPC	Information and Privacy Commissioner
NWT	Northwest Territories
OIPC	Office of the Information and Privacy Commissioner
PHA	*Public Health Act*
PHI	Personal Health Information
PHIPA	Ontario's *Personal Health Information Protection Act, 2004*
PIA	Privacy Impact Assessment
PIPEDA	*Personal Information Protection and Electronic Documents Act* (Canada)


10 YEAR

Executive Summary

The Northwest Territories' *Health Information Act* (HIA) came into force on October 1, 2015. The Department of Health and Social Services (DHSS) is responsible for implementing and monitoring the HIA in NWT. The purpose of this ten-year report is to provide an overview that:

- Responds to the requirement under section 195.1 of the HIA to review the Act no later than 10 years after the Act came into force.
- Provides an update on HIA implementation activities and compliance status from October 2015 to April 2025.
- Summarizes a general status review of the HIA that includes experience and issues with implementing HIA over the last 8-10 years, and a table of conclusions and recommendations.

This review gathered issues that the health and social services system (HSS) has been made aware of and identifies considerations for future in-depth study and potential amendment. The report touches on emerging issues such as indigenous data sovereignty, data stewardship, and how new technologies in the digital healthcare landscape introduce evolving complexities in health privacy.

DHSS determined that a general status review conducted through existing resources was the appropriate approach to this first review. This was influenced by the following critical factors: financial constraints; recognition that the HIA is the first piece of legislation of its kind enacted in the NWT; complexity of the legislation, the importance of suitable skill set and subject matter expertise facilitating the efforts; and alignment with and relevance to the NWT context.

The legislation is assessed as functional; however, areas of work have been identified for further consideration. The table below summarizes the conclusions made throughout the document. The conclusions are listed in order of the HIA parts and sections. In summary, the conclusion of this report is that more work is required to determine the next steps for appropriate legislative amendment.

Topics for Consideration	Conclusions / Considerations	Recommendations
HIA PART 1 – INTERPRETATION AND APPLICATION		
• Adding new terms into definitions	Each submission from the invested organizations on proposed changes to existing definitions or introducing new terms would benefit from completing an assessment from the 'value added' perspective and its substantiation when measuring beneficial impact on ongoing improvements of the HIA and its interpretation.	More work and engagement for appropriate legislative amendment.
HIA PART 2 – ROLES AND RESPONSIBILITIES		
• Adding other health care professionals as health information custodians	Additional health information custodians can be added as needed to the Regulations. Policy work is needed to determine which additional custodians should be added.	More work and engagement for appropriate legislative amendment.
• Custodians that are not employed by the GNWT are not aware they are custodians and subject to the HIA	The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution. Additional private health information custodians can be added as needed to the Regulations. More policy work is needed to determine if an exhaustive list of custodians is desired, and which private custodians should be added.	A policy tool should be developed.

• Public Guardian to be considered as a custodian	The issue lies not with the legislative framework of the HIA but with the position of the Public Guardian within the DHSS. Policy work is needed to determine whether amendments to the HIA or the *Guardianship and Trusteeship Act* would be most appropriate.	More work and engagement for appropriate legislative amendment.
HIA PART 3 – CONSENT AND SUBSTITUTE DECISION MAKERS		
• Mature minor consent when addressing complex issues (age indication for mature minor)	The HIA is aligned with common law in other jurisdictions in Canada, however other resources and training should be considered to assist custodians to guide assessment of minors' maturity.	A policy tool should be developed.
• The consent section is long and complex	The length of the consent part is in line with other Canadian jurisdictions. Policy work should be done to see if these sections of the HIA can meaningfully be simplified.	A policy tool should be developed.
• Some HIA provisions cannot be implemented with existing resources (consent conditions)	Amending the HIA will not solve the use of consent conditions in a particular eHealth system. Funding by the GNWT for system enhancement is outside of the scope of legislation.	N/A
HIA PART 4 – COLLECTION, USE, DISCLOSURE AND PROTECTION OF PHI		
• Use of mobile devices to disclose images for consultation	The current HIA adequately addresses the use and disclosure of patient photographs for consultation purposes. The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution.	A policy tool should be developed.

• Collection/Use/Disclosure of PHI for Cancer Surveillance Program	While the intent of the Territorial Cancer Surveillance program is aligned with preventative health objectives, the current provisions of the HIA and Regulations do not clearly permit the collection, use and disclosure of PHI for the purpose of directly contacting average-risk individuals for cancer screening. Consideration could be given to amend the HIA Regulations to include a specific provision authorizing the disclosure of PHI for the purposes of organized population-based screening programs.	More work and engagement for appropriate legislative amendment.
• Disclosure of PHI for joint Guardianship and Trusteeship applications	The current legislative framework creates practical and legal challenges in preparing joint guardianship and trusteeship applications due to limits on the disclosure of personal health information. Amending the *Guardianship and Trusteeship Act* would more directly and effectively address the issue of PHI disclosure in this context, ensuring timely and lawful access to necessary information. However, consideration could also be given to amending the HIA to permit limited, purpose-specific disclosure where doing so would benefit the client.	More work and engagement for appropriate legislative amendment.

• Disclosure of PHI to the NWT Leadership Council	Under HIA, there is no authority for health information custodians to disclose identifiable PHI to the NWT Health and Social Services Leadership Council without consent. However, the Council's oversight and advisory role can be fully supported using de-identified information.	No further work is needed.
• Disclosure of PHI to other government bodies	Under the current HIA, health information custodians are not authorized to disclose identifiable PHI to ECE or EIA for schools, income support, or integrated service delivery purposes without the individual's consent. More policy work is needed to identify the scope of policy or legislative amendments to appropriately target such a disclosure for these purposes. Other Canadian jurisdictions have addressed this issue through targeted amendments and multi-agency frameworks that balance service integration with privacy protections.	More work and engagement for appropriate legislative amendment.
• Jurisdictional Clarification of Section 50(b) of HIA	Section 50(b) of the HIA would benefit from a legislative amendment in the future to explicitly state that only subpoenas, warrants, and legal orders enforceable within NWT jurisdiction authorize the disclosure of PHI without consent. This would align the HIA with best practices in jurisdictions like Alberta and provide certainty to custodians.	A policy tool should be developed.

	As a secondary option, in the absence of an amendment, custodians should adopt a formal policy or SOP requiring verification of jurisdictional validity before disclosing PHI in response to legal instruments. This would help ensure lawful disclosure, support consistent decision-making, and uphold the privacy principles underlying the HIA.	
• Managing Public Health Outbreaks and Duty of Care	The *HIA and Public Health Act* PHA in the NWT provide a legally sufficient and nationally aligned framework for the disclosure and use of PHI during public health outbreaks such as measles. Disclosure to public health officials is authorized without consent under Section 66 of the HIA, referencing the clear authority granted under the PHA. Furthermore, physicians may access the immunization status of their patients as part of providing care and are ethically obligated, under the duty of care, to use that information to protect patients' health. The existing legislative framework aligns with other Canadian jurisdictions and adequately supports both public health surveillance and clinical responsibilities.	There is no demonstrated requirement to amend the HIA to support these functions. Amendments to PHA would require separate consideration.

• Public Health Surveillance	The current legal framework allows for the disclosure of PHI to the Chief Public Health Officer under section 35 of the *Public Health Act* for public health surveillance of chronic diseases without individual consent, provided: • There are reasonable grounds for the collection, • The amount of data is limited to what is necessary, and • The custodian agrees to provide the information. However, the lack of a statutory definition of public health surveillance in HIA may contribute to uncertainty about the scope of such disclosures. Consideration could be given to amending the legislation to include an express definition of public health surveillance in future amendments to enhance clarity.	More work and engagement for appropriate legislative amendment.
HIA PART 5 – ACCESS TO AND CORRECTION OF PERSONAL HEALTH INFORMATION		
HIA PART 6 – REVIEW AND APPEAL		
HIA PART 7 – INFORMATION AND PRIVACY COMMISSIONER		
• Extend time for health information custodian response to IPC's recommendation from 30 days to 90 days.	These IPC recommendations to change the timelines are being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.	More work and engagement for appropriate legislative amendment.
• Extend time to comply with a decision from 45 days to 90 days.		
• HIA to define 'days' to 'business days'.		

• Reporting privacy breaches to the IPC (harms test)	The introduction of a harms test for breach notification does have precedence in other Canadian jurisdictions. However, any proposed changes to the legislation introduces legal, ethical, and practical risks, when compared to the current mandatory reporting model, and should be carefully considered to ensure accountability by custodians and maintaining public confidence.	
• Section 153- Powers of IPC	These IPC recommendations regarding processes are still being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.	
• Section 158 – Requirement to comply with decision		
• Section 134 – Request for review		
• Section 89(2) and Section175 – Privacy impact assessment	Tools such as policy amendment or a procedure able to provide more clarity for PIA stages are being considered. Relevant invested organizations, including Office of the IPC, DHSS and HSSAs would be valuable resources to inform these tools.	A policy tool should be developed.

HIA PART 8 – GENERAL		
• Addition of a 'snooping' offence	The act of snooping in sensitive PHI by employees in a position of trust is an abuse of power and can significantly erode trust in the health care system. To align with other jurisdictions in Canada, and to recognize the seriousness of snooping activity, consideration should be given to introducing a separate clause in the HIA to criminalize intentional unauthorized access to health records with proportionate penalties. Additional consideration of administrative monetary penalties as a potential enforcement mechanism should be reviewed.	More work and engagement for appropriate legislative amendment.

NWT *Health Information Act* Ten Year Review Report / October 2025
Rapport sur l'examen décennal de la *Loi sur les renseignements sur la santé* des TNO | Octobre 2025

10 YEAR

Sommaire

La Loi sur les renseignements sur la santé (LRS) est entrée en vigueur le 1er octobre 2015. Aux TNO, le ministère de la Santé et des Services sociaux (MSSS) est responsable de mettre en œuvre la Loi et d'en surveiller l'application. Le présent rapport décennal vise à fournir un aperçu qui :

- Répond à l'exigence énoncée à l'article 195.1 de la LRS, qui prévoit qu'un examen de la Loi doit être réalisé au plus tard dix ans après son entrée en vigueur;
- Fait le point sur la conformité et l'application de la Loi pour la période allant d'octobre 2015 à avril 2025;
- Brosse un bilan général de la LRS, lequel comprend l'expérience acquise et les problèmes liés à sa mise en œuvre au cours des huit à dix dernières années, ainsi qu'un tableau présentant les conclusions et les recommandations.

Le présent examen a permis de recenser les problèmes connus du système de santé et des services sociaux et de cerner des éléments dans la Loi qui devront faire l'objet d'une étude approfondie et possiblement être modifiés. Le rapport aborde également de nouveaux enjeux, notamment la souveraineté des données autochtones, la gestion des données et les défis croissants en lien avec la protection de la vie privée, qui découlent de l'utilisation de nouvelles technologies dans le domaine de la santé numérique.

Le MSSS a déterminé qu'une révision générale de la Loi réalisée à l'aide des ressources en place constituait l'approche la plus appropriée pour ce premier examen. Les contraintes financières, la reconnaissance du fait que la LRS est la première loi de ce genre adoptée aux TNO, la complexité de la Loi, l'importance de disposer de compétences appropriées et d'une d'expertise spécialisée pour soutenir sa mise en œuvre, et la nécessité de l'adapter au contexte particulier des TNO ont largement contribué à cette décision.

Si la Loi est jugée fonctionnelle, certains domaines semblent toutefois nécessiter un examen plus approfondi. Le tableau ci-dessous résume les conclusions tirées tout au long du document. Elles sont présentées selon l'ordre des parties et des articles de la LRS. En conclusion, le rapport établit que des travaux supplémentaires sont nécessaires afin de déterminer les prochaines étapes en vue d'effectuer les modifications législatives qui s'imposent.

Points à considérer	Conclusions et points à considérer	Recommandations
PARTIE 1 DE LA LRS – INTERPRÉTATION ET CHAMP D'APPLICATION		
• Ajout de nouveaux termes aux définitions	Chaque présentation des organismes concernés portant sur des modifications proposées aux définitions existantes ou sur l'introduction de nouveaux termes gagnerait à inclure une évaluation fondée sur la valeur ajoutée, ainsi qu'une justification démontrant les retombées positives attendues sur l'amélioration continue de la LRS et sur son interprétation.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.
PARTIE 2 DE LA LRS – RÔLES ET RESPONSABILITÉS		
• Ajout d'autres professionnels de la santé à titre de dépositaires de renseignements sur la santé	D'autres dépositaires de renseignements sur la santé peuvent être ajoutés au Règlement, au besoin. Des politiques doivent être créées afin de déterminer quels dépositaires additionnels devraient figurer au Règlement.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.

• Les dépositaires qui ne sont pas employés par le GTNO ne savent pas qu'ils sont des dépositaires et qu'ils sont assujettis à la LRS	Le problème relève davantage de la mise en œuvre de la Loi et du respect des exigences que du cadre législatif établi. Renforcer la formation ainsi que l'application des politiques et des procédures constitue la solution la plus efficace et la plus équilibrée. Des dépositaires privés de renseignements sur la santé peuvent être ajoutés au Règlement, au besoin. Des travaux supplémentaires sur les politiques sont nécessaires pour déterminer s'il est souhaitable d'établir une liste exhaustive des dépositaires, et pour préciser les dépositaires privés à ajouter.	L'élaboration d'une politique serait nécessaire.
• Le tuteur public à considérer comme dépositaire	Le problème relève davantage du statut du tuteur public au sein du MSSS que du cadre législatif établi. Des travaux sur les politiques sont nécessaires afin de déterminer s'il serait plus approprié d'apporter des modifications à la LRS ou à la *Loi sur la tutelle.*	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.
PARTIE 3 DE LA LRS – CONSENTEMENT ET SUBROGÉS		
• Consentement des mineurs matures dans des situations complexes (indication de l'âge applicable)	La LRS est conforme aux lois d'autres administrations canadiennes. Il serait toutefois pertinent de fournir des ressources et de la formation supplémentaires afin d'aider les dépositaires à évaluer la capacité des mineurs.	L'élaboration d'une politique serait nécessaire.

• La section sur le consentement est longue et complexe	La longueur de la section portant sur le consentement est comparable à celle d'autres administrations canadiennes. Des travaux sur les politiques devraient être menés afin de déterminer si ces dispositions de la LRS peuvent être simplifiées pour en faciliter la compréhension.	L'élaboration d'une politique serait nécessaire.
• Certaines dispositions de la LRS ne peuvent pas être mises en œuvre avec les ressources actuelles (consentement)	Modifier la LRS ne permettra pas de régler la question de la nécessité d'obtenir le consentement dans un système de santé en ligne donné. Le financement du GTNO pour l'amélioration des systèmes dépasse le champ d'application de la Loi.	S. O.
PARTIE 4 DE LA LRS – COLLECTE, UTILISATION, DIVULGATION ET PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ		
• Utilisation d'appareils mobiles pour la communication d'images à des fins de consultation	La LRS actuelle encadre adéquatement l'utilisation et la communication de photographies de patients à des fins de consultation. Le problème tient davantage à la mise en œuvre de la Loi et au respect des exigences qu'au cadre législatif établi. Renforcer la formation ainsi que l'application des politiques et des procédures constitue la solution la plus efficace et la plus équilibrée.	L'élaboration d'une politique serait nécessaire.

• Collecte, utilisation et divulgation de renseignements personnels sur la santé pour l'application du Programme de surveillance du cancer	Bien que l'objectif du Programme de surveillance du cancer des TNO soit conforme aux objectifs de prévention en santé, les dispositions actuelles de la LRS et de son règlement ne permettent pas expressément la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé aux fins de communication directe avec des personnes qui présentent un risque moyen et qui devraient se faire dépister. Il pourrait être envisagé de modifier le Règlement afin d'y inclure une disposition qui autoriserait la divulgation de renseignements personnels sur la santé pour les programmes de dépistage organisés à l'échelle de la population.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.
• Divulgation de renseignements personnels sur la santé dans le cadre de demandes conjointes de tutelle	Le cadre législatif actuel pose des difficultés pratiques et juridiques lors de la préparation de demandes conjointes de tutelle en raison des limites imposées à la divulgation de renseignements personnels sur la santé. La modification de la Loi sur la tutelle permettrait de traiter cette question de manière plus directe et plus efficace, en permettant d'accéder aux renseignements nécessaires en temps opportun et de façon tout à fait légale. Il pourrait toutefois être envisagé de modifier la LRS afin de permettre la divulgation des renseignements dans certains cas précis, notamment dans les situations où le partage des informations sur la santé est dans l'intérêt du client.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.

• Divulgation de renseignements personnels sur la santé au Conseil de leadership des Territoires du Nord Ouest	En vertu de la LRS, les dépositaires de renseignements sur la santé ne sont pas autorisés à divulguer au Conseil de leadership des services de santé et des services sociaux des TNO des renseignements personnels sur la santé d'une personne qui permettraient de l'identifier sans son consentement. Toutefois, le Conseil peut exercer pleinement son rôle de supervision et son rôle consultatif en utilisant les renseignements anonymisés.	Aucune autre mesure n'est requise.
• Divulgation de renseignements personnels sur la santé à d'autres organismes gouvernementaux	En vertu de la LRS actuelle, les dépositaires de renseignements sur la santé ne sont pas autorisés à divulguer, sans le consentement de la personne concernée, des renseignements personnels sur la santé en lien avec l'éducation, le soutien au revenu ou la prestation intégrée de services qui permettraient de l'identifier auprès de certains organismes (MECF ou MEAA). Des travaux supplémentaires sur les politiques sont nécessaires afin de définir la portée des modifications stratégiques ou législatives requises pour encadrer adéquatement une telle divulgation. D'autres administrations canadiennes ont effectué des modifications ciblées et établi des cadres interorganismes qui permettent de concilier intégration des services et protection de la vie privée.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.

• Clarification de la compétence à l'alinéa 50b) de la LRS	L'alinéa 50b) de la LRS gagnerait à être modifié pour préciser que seuls les mandats, les assignations et les ordonnances judiciaires exécutoires aux TNO peuvent permettre la divulgation de renseignements personnels sur la santé sans le consentement de la personne visée. Une telle modification permettrait d'aligner la LRS sur les pratiques exemplaires observées dans d'autres administrations, comme l'Alberta, et offrirait une plus grande certitude aux dépositaires. Si la Loi n'est pas modifiée, les dépositaires devraient adopter une politique officielle ou une procédure opérationnelle normalisée afin d'exiger que soit vérifiée la force exécutoire des instruments juridiques aux TNO avant de divulguer des renseignements personnels sur la santé. Cette approche contribuerait à assurer que les informations soient partagées conformément à la Loi, à favoriser une prise de décision uniforme et à respecter les principes de protection de la vie privée qui sous-tendent la LRS.	L'élaboration d'une politique serait nécessaire.

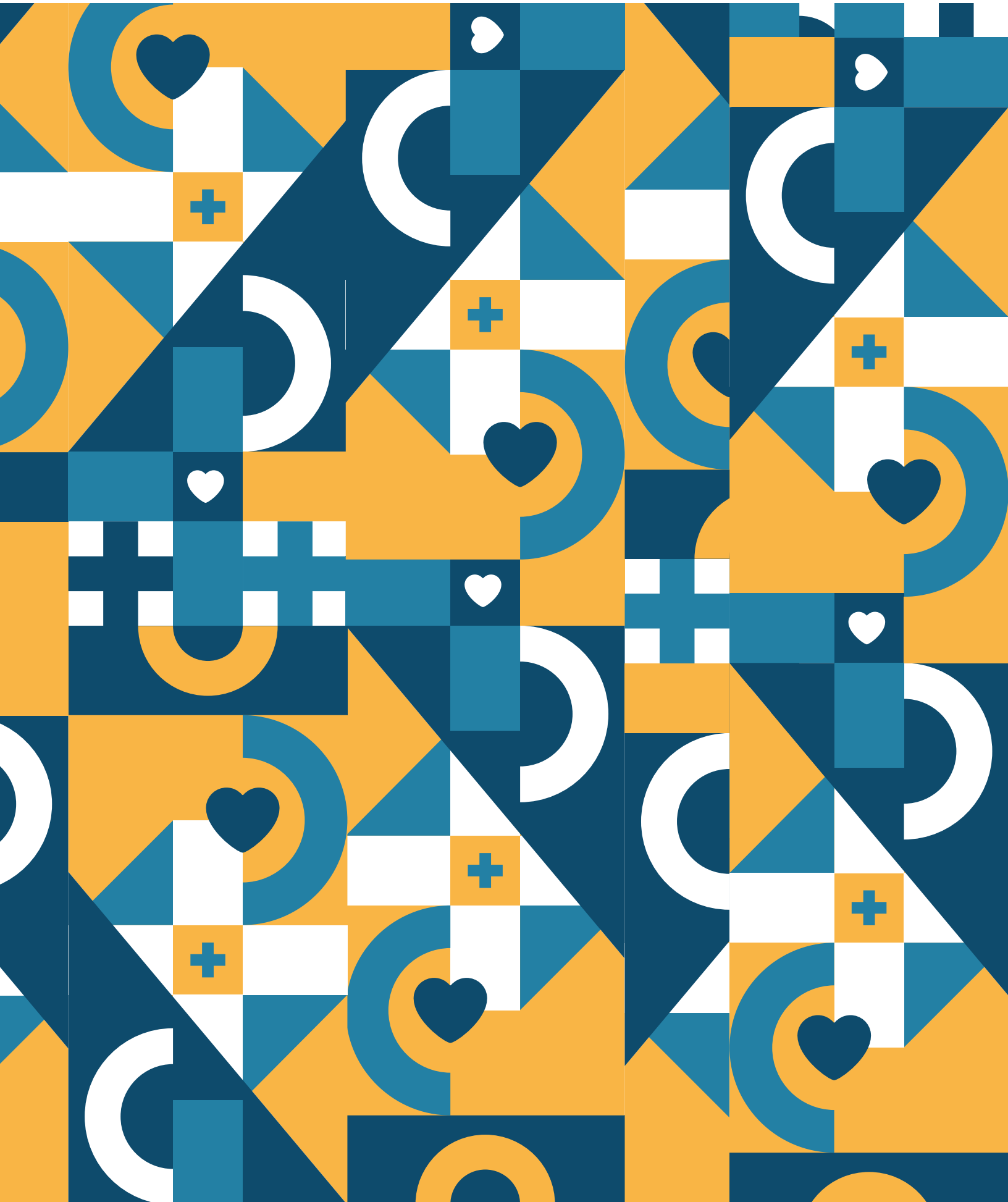
• Gestion des cas d'éclosions menaçant la santé publique et devoir de diligence	Aux TNO, la LRS et la *Loi sur la santé publique* offrent un cadre juridique suffisant qui est conforme à celui qu'on retrouve à l'échelle nationale en ce qui a trait à l'utilisation et à la divulgation de renseignements personnels sur la santé lors d'éclosions qui menacent la santé publique, par exemple dans les cas d'éclosion de rougeole. La divulgation de renseignements aux autorités de santé publique est autorisée sans le consentement de la personne visée en vertu de l'article 66 de la LRS, lequel renvoie aux pouvoirs clairement conférés par la *Loi sur la santé publique*. De plus, les médecins peuvent accéder au statut vaccinal de leurs patients dans le cadre de la prestation de soins. Ils ont le devoir moral et professionnel d'utiliser ces informations pour protéger la santé des patients. Le cadre législatif actuel est conforme à celui d'autres administrations canadiennes et soutient adéquatement tant la surveillance en santé publique que les responsabilités cliniques.	Rien ne justifie la modification de la LRS pour remplir ces fonctions. Toute modification à la *Loi sur la santé publique* nécessiterait un examen distinct.

• Surveillance de la santé publique	En vertu de l'article 35 de la *Loi sur la santé publique*, la divulgation de renseignements personnels sur la santé sans le consentement de la personne concernée à l'administrateur en chef de la santé publique est permise à des fins de surveillance des maladies chroniques. Il faut toutefois que les conditions suivantes soient réunies : • il existe des motifs raisonnables justifiant la collecte; • les renseignements divulgués sont limités à ce qui est nécessaire; • le dépositaire consent à fournir les renseignements. L'absence d'une définition de la surveillance de la santé publique dans la LRS peut créer de l'incertitude quant à ce qui peut être partagé légalement. Si des modifications étaient apportées à la Loi, on pourrait envisager d'y ajouter une définition claire.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.

PARTIE 5 DE LA LRS – RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ : ACCÈS ET CORRECTION PARTIE 6 DE LA LRS – RÉVISION ET APPEL PARTIE 7 DE LA LRS – COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE		
• Faire passer de 30 jours à 90 jours le délai accordé aux dépositaires de renseignements sur la santé pour répondre aux recommandations du Commissaire à l'information et à la protection de la vie privée	Ces recommandations du Commissaire à l'information et à la protection de la vie privée visant à modifier les délais font actuellement l'objet d'une évaluation afin d'en mesurer les répercussions sur l'ensemble de la LRS. Elles pourraient être proposées ultérieurement dans le cadre du processus de modification de la Loi.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.
• Faire passer de 45 jours à 90 jours le délai pour se conformer à une décision		
• Préciser dans la LRS que le terme « jours » s'entend de « jours ouvrables »		
• Déclaration des atteintes à la vie privée au Commissaire à l'information et à la protection de la vie privée (critère du préjudice)	L'ajout d'un critère du préjudice pour la déclaration des atteintes à la vie privée trouve des précédents dans d'autres administrations canadiennes. Toutefois, toute modification proposée à la Loi comporte des risques juridiques, éthiques et pratiques lorsqu'on la compare au modèle actuel de déclaration obligatoire. Ces changements devraient donc être examinés avec soin afin de s'assurer que l'obligation de rendre compte des dépositaires est garantie et que la confiance du public est maintenue.	

• Article 153 – Pouvoirs du commissaire • Article 158 – Obligation de se conformer à la décision • Section 134 – Demande de révision	Ces recommandations du Commissaire à l'information et à la protection de la vie privée concernant les processus font toujours l'objet d'une évaluation afin d'en mesurer les répercussions sur l'ensemble de la LRS. Elles pourraient être proposées ultérieurement dans le cadre du processus de modification de la Loi.	
• Paragraphe 89(2) et article 175 – Évaluation des répercussions sur la vie privée	Des modifications aux politiques ou l'élaboration de procédures visant à clarifier les étapes des évaluations des facteurs relatifs à la vie privée sont à l'étude. Les organismes concernés, dont le Bureau du Commissaire à l'information et à la protection de la vie privée, le MSSS et les administrations des services de santé et des services sociaux, constitueraient des ressources précieuses pour éclairer l'élaboration de ces outils.	L'élaboration d'une politique serait nécessaire.

PARTIE 8 DE LA LRS – DISPOSITIONS GÉNÉRALES		
• Ajout d'une infraction liée à l'accès non autorisé (« espionnage »)	La consultation sans autorisation des renseignements personnels sur la santé (« espionnage ») par des employés occupant un poste de confiance constitue un abus de pouvoir et peut éroder de façon importante la confiance du public envers le système de soins de santé. Dans le but de s'aligner sur les pratiques d'autres administrations canadiennes et de reconnaître la gravité de tels comportements, il pourrait être envisagé d'ajouter à la LRS une disposition érigeant en infraction l'accès intentionnel et non autorisé aux dossiers de santé, et imposer des peines proportionnelles. Il conviendrait également d'examiner la possibilité d'introduire des sanctions administratives pécuniaires comme mécanisme d'application de la Loi.	Davantage de travaux et d'échanges sont requis pour apporter les modifications nécessaires à la Loi.



TEN-YEAR REPORT ON THE NORTHWEST TERRITORIES *HEALTH INFORMATION ACT*

ACKNOWLEDGEMENT

The working group was established from internal DHSS resources, consisting of four staff with expertise in health privacy and two staff providing legislative and legal input. Acknowledgement and appreciation are provided to the following individuals for invaluable work and contributions in this report:

1. Livia Kurinska-Hrdlickova, Chief Health Privacy Officer
2. Jennifer Howie, ATIPP and Health Privacy Officer
3. Tanya Krueger, Senior Privacy Specialist
4. Taryl Gula, Senior Health Privacy Officer
5. Dana Webster, Senior Policy Analyst
6. Alexander Canuel-Kirkwood, Policy Analyst

The identified members of the working group were well positioned to complete this work because many of them had been involved with the HIA implementation efforts since 2015, have valuable hands-on experience, and are front-line staff receiving feedback and solving day-to-day challenges responding to public inquiries. To help inform this report, the working group completed a cross-jurisdictional scan of all provinces and Yukon's equivalent health information legislation. British Columbia and Nunavut do not have personal health information legislation at the time of writing this report.

ABOUT THIS REPORT

This report is structured into four parts:

- Part 1 of the report provides background information on the original goals and objectives for the HIA, and explains implementation efforts, compliance status and DHSS ongoing responsibilities.
- Part 2 contains seven sections; each begins with a summary of relevant sections from the HIA to support a comprehensive and clear understanding of the challenges followed by feedback from invested organizations along with a discussion where relevant background context or research findings are presented and considered for the HSS context. Finally, each section concludes with considerations of how to address the presented issue or challenge.
- Part 3 brings forward new emerging themes which occurred since HIA came into force in the NWT and to be considered in shaping future versions of HIA. Emerging trends and technological advancements keep impacting the collection, use, disclosure, access and retention of personal health information.
- Part 4 presents a summary of all considerations for future legislative amendments.

Part 1 - Introduction And Compliance Overview

Preparation of this ten-year review report involved summarizing and analyzing a decade worth of implementation efforts and compliance status with HIA. This method allowed us to report on the current state, what the experience has been to this point, issues encountered, and what else to consider in the future.

1.1 ENGAGEMENT PROCESS

The review commenced in February 2023 by DHSS formulating a path to the ten-year legislative report. The experience and issues with implementing HIA were drawn from feedback provided by invested organizations, which has been collected by DHSS on an ongoing basis since 2015. The DHSS Health Privacy team has also been meeting on an as-needed basis with the invested organizations on specific issues. Call outs for any additional remaining feedback to be considered for the purposes of this report were requested. Further details on engagement with invested organizations are set out below in Table 1.

TABLE 1 - ENGAGEMENT AUDIENCE

Engagement audience (invested organizations)	Date of engagement	Type of engagement conducted
Health and Social Services Authorities (HSSA) • Hay River HSSA • Tłı̨chǫ Community Services Agency • Northwest Territories HSSA	August 6, 2024 Oct 2015 – Aug 2024	Call out for written submissions Ongoing written submissions
Office of the NWT Information and Privacy Commissioner	August 6, 2024 November 8, 2024 March 19, 2025 Oct 2015-Aug 2024	Call out Meeting Letter Ongoing written submissions through formal recommendations and letters
Department of Health and Social Services • departmental divisions	October 9, 2024 Oct 2015 – Oct 2024	Call out Ongoing written submissions

1.2 BACKGROUND

The Northwest Territories (NWT) *Health Information Act* (HIA) came into force on October 1, 2015. The purpose of the HIA is to recognize both individuals' rights to access and correct their own information and the needs of heath service providers to collect, use, and disclose personal health information to provide health care. Penalties may be imposed if the rules of the HIA are not followed.

The foundation and spirit of the HIA was rooted in health privacy principles, supported by regulatory guidance and the ability to remain effective in anticipation of future technological advancements. Privacy principles control the amount and type of information that is collected, used and disclosed. The privacy principles are:

- Collect, use and disclose only the least amount of information necessary;
- Collect, use and disclose identifiable information only when non-identifiable won't do;
- Know why this information is needed now.

In implementing the HIA, DHSS became the territory-wide lead on health privacy. A Health Privacy Office was established at DHSS, which is responsible for raising privacy awareness, and enforcement and promotion of the HIA in the NWT.

The Health Privacy Office goals and objectives listed below are aligned to support the broader priorities of DHSS for an accountable health and social services system:

GOALS

1. The health and social services system has a strong privacy framework;
2. The health and social services system has a strong privacy culture and privacy awareness;
3. The health and social services system is compliant with the privacy and records management framework;
4. Health Privacy Office has strong relationships with key invested organizations to affect change management and strengthen privacy; and
5. The health and social services system privacy framework is consistent with best practices elsewhere in Canada.

OBJECTIVES

1. Strengthen the privacy framework (to achieve Goal 1);
2. Develop and deliver privacy and records management supports (to achieve Goals 2,3,4);
3. Carry out compliance activities (to achieve Goal 3);
4. Proactively influence invested organizations (to achieve Goal 4);
5. Listen to and help invested organizations in a way that helps promote privacy (to achieve Goal 4); and
6. Provide knowledge translation of privacy best practices to invested organizations (to achieve Goal 5).

1.3 IMPLEMENTATION AND COMPLIANCE STATUS (OCTOBER 2015 – APRIL 2025)

DHSS has been leading implementation activities since October 2015. DHSS Health Privacy team receives feedback on an ongoing basis related to HIA compliance and provides guidance on administration and enforcement of the HIA to the DHSS, HSSAs, and physicians and pharmacists who are not employed by the custodians within the GNWT. The compliance activities are guided by recommendations issued by the IPC and on-going feedback. The following activities were carried out:

- Updated Ministerial Directive for privacy and security policies that apply to DHSS and HSSAs. The following privacy and security policies were added or updated as of the date indicated:
    - Consent Conditions Policy (2025) – introduces a consistent process across the HSS to respect, acknowledge, follow, and appropriately document consent conditions requested by individuals or substitute decision makers;
    - Contractor Compliance Policy (2017) – identifies reasonable measures that must be taken to ensure that personal health information is protected when a contractor is providing a service on behalf of DHSS or HSSAs;
    - Electronically Stored and Transferred Information Policy (2019) – provides a consistent approach that ensures safe and secure storage and transfer of electronic information;
    - Recording Device Policy (2023) – provides a consistent approach that ensures the DHSS and HSSAs comply which the HIA when a recording device is used that collects and records personal health information in a manner that may not be obvious to the individual whose information is being collected;
    - Withdrawing Consent Policy (2023) – establishes a consistent process across the HSS to respect, acknowledge, follow, and appropriately document withdrawal of consent requested by individuals or substitute decision makers.

The development of the following policies is underway:

- Auditing policy
- Electronic information system access management policy
- Release of information policy, with appendix guidelines for:
    - Accessing minor/mature minor information
    - Family of deceased's right to information
    - Record of disclosure
    - Client recording /Use of recording device (recording) by clients
- Supported HSSAs on development and implementation of their privacy and security policies
- Provided privacy advice on an ad-hoc basis to private pharmacists and private physicians

Factors that impacted timely progress on implementation efforts and compliance gaps during 2015-2025:

- Staffing issues (turnover/retention) within DHSS and HSSAs related to the privacy teams having subject matter experts available;
- Response to Covid-19 impacted implementation efforts - the pandemic raised the need to implement many technologies and tools at a rapid speed with technology playing a central role.

Some of the planned implementation efforts were paused, while transitioning to work remotely and complying with public health guidelines. Focus was redirected to providing privacy input and advisory work for Covid-19 initiatives and processes. Although the Covid-19 Coordinating Secretariat dissolved on April 1, 2022, DHSS continued managing privacy matters pertaining to Covid-19 Coordinating Secretariat, including management of HIA privacy breach files until the end of 2024.

1.3.1 COMPLIANCE

Compliance with HIA requires DHSS to continuously review all electronic systems related to the handling of personal health information, through risk and privacy impact assessments to ensure alignment with the privacy legislation, and necessary security and privacy practices. Monitoring systems development and operations for security and privacy ensures that the use of technologies maintains reasonable privacy safeguards and protection on collection, use, disclosure and access of personal health information within. The DHSS Health Privacy team monitors changes in healthcare laws and regulations through participating in privacy related pan-Canadian committees and by assessing the impact on the HSS to inform future updates of privacy programs and policies.

The DHSS carried out the following compliance activities from October 2015 – April 2025:

- Prepared and completed review of forty [40] privacy impact assessments (PIA), some of the work involved supporting HSSAs conducting their PIAs.
- Assessed and updated forms, information sharing agreements, information management agreements and research agreements to comply with the HIA obligations.
- Considered HIA privacy obligations, where applicable, during renewal of existing service agreements and contracts.
- Participated and collaborated with the NWT Research Ethics Committee.
- Ensured DHSS and HSSAs have designated contact persons appointed as required under the HIA.
- Responded to one hundred and forty-three [143] general HIA inquiries received via the HIA email address (HIA@gov.nt.ca) from the public and staff.
- Received and processed seventy-one [71] requests from clients for a 'Record of Activity' from a designated eHealth information system.
- Ensured ongoing auditing and monitoring of e-Health information systems designated under the HIA.

In 2016, the DHSS and HSSAs established a Territorial HSS Privacy Advisory Committee (HSS PAC), attended by privacy representatives from each organization, and chaired by DHSS Health Privacy lead. HSS PAC strengthens the territorial health privacy framework by promoting the integration of privacy best practices in the delivery and administration of health and social services; and serves as a networking platform for health privacy experts to review and analyze any patterns in privacy incidents, share privacy tools, exchange advice, and identify and assist with the resolution of privacy matters.

[1]https://www.hss.gov.nt.ca/sites/hss/files/resources/know-your-privacy-rights.pdf

The Table 2 below provides a summary of health information privacy breaches across the health system between October 2015 to April 2025 that were investigated, confirmed and mitigated.

TABLE 2

Organization	Number of privacy breaches under the HIA
DHSS	44
Covid-19 Coordinating Secretariat*	51
HRHSSA	70
TCSA	34
NTHSSA	574

*CS-19 (dissolved on April 1, 2022) privacy breaches were managed under DHSS

The number of breaches between 2020 and 2023 were significantly higher due to several factors such as staff redeployment in response to the pandemic, new electronic systems and workflows introduced in rapid response to the pandemic, and high work volume with long staff hours.

1.3.2. TRAINING

Training is essential in understanding the importance of confidentiality and privacy when handling personal health information. New staff receive mandatory privacy training as part of the orientation process which is required to be renewed annually.

DHSS is responsible for creating and maintaining all health privacy training material for DHSS and HSSAs to ensure consistent messaging and training. Provision of training sessions is the responsibility of each organization. DHSS and HSSAs must each maintain a central record of attendance.

The current privacy and HIA training are tailored for staff, dependent on job duties and the amount of information they deal with. See Table 3 – Privacy and HIA Training Modules.

Training is delivered through several methods such as a live-facilitator session, self-paced or one-on-one for a specific topic. Self-paced training is available on the GNWT Enterprise Learning Management System, providing additional flexibility for staff to review the privacy training materials, while allowing them to pause and resume at their own schedule.

Using evaluation criteria designed to ensure training tools are effective, DHSS continuously gathers feedback from training participants and HSSAs. Between October 2015 to April 2025 one hundred seventy-five [175] privacy training evaluation responses were collected from staff and contractors that informed updates on the training content.

Privacy news and updates are communicated with DHSS and HSSA staff on a regular basis. Other strategies adopted by DHSS and HSSAs to promote general privacy awareness and education within HSS departments include:

- Staff are provided with access to Health Information Act Guide- https://www.hss.gov.nt.ca/sites/hss/files/hia-guide.pdf and relevant resources to assist with education on privacy obligations.
- Privacy issues are identified and addressed during development and implementation of any new communications and information systems and programs.
- Highlighting staff privacy obligations during Data Privacy Day and Privacy Awareness Month activities.
- Designated Contact Persons across DHSS and HSSAs provide tailored advice to staff to support them in understanding and meeting their privacy obligations. For example, the Designated Contact Person can provide advice about:
  - Whether personal or personal health information is being collected, used, or disclosed for a lawful purpose;
  - Whether collection of personal health information is reasonably necessary for the specified purpose;
  - Whether any exemptions apply;
  - How to manage breaches, complaints, requests from the Office of the Information and Privacy Commissioner (OIPC).
- Liaising with the OPIC and GNWT Office of the Chief Information Officer.
- Conducting privacy impact assessments to help staff to identify and minimize privacy risks when starting a new initiative or making changes to existing initiatives.

TABLE 3

PRIVACY & HIA TRAINING MODULES OVERVIEW BY JOB AREA

JOB AREA with Information Handling	Handling general information ONLY (not handling personal and/or personal health information)	Handling personal information	Using electronic information system(s) with personal information	Handling personal health information	Using electronic health information system(s)	Records management / access request processing	Quality Risk Management	Responsible for HIA legislative compliance
TRAINING MODULES	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality	General Privacy and Confidentiality
		Respecting Patient/ Client Privacy	Respecting Patient/ Client Privacy	HIA Overview	HIA Overview	HIA Overview	HIA Overview	HIA Overview
		Privacy Safeguards	E-Privacy (admin or user)	Respecting Patient/ Client Privacy	Respecting Patient/ Client Privacy	Respecting Patient/ Client Privacy	Respecting Patient/ Client Privacy	Respecting Patient/ Client Privacy
				Privacy Safeguards	Privacy Safeguards	Privacy Safeguards	Privacy Safeguards	Privacy Safeguards
					E-Privacy (admin or user)	Access & Correction	Incident Investigation & Privacy Breach	Incident Investigation & Privacy Breach
						Complex Consent	Complex Consent	Access & Correction
								HIA Designated Contact Person Responsibilities
								Complex Consent
								Train the Trainer & Refresh

Optional Training Modules

- Research
- Health System Planning
- Privacy Impact Assessment
- Privacy by Design / Privacy Requirements for new projects
- Privacy Brown Bag Lunches on policies, tools, and best practices

MANDATORY | **MANDATORY DUTIES DEPENDENT** | **OPTIONAL**

1.3.3. PUBLIC AWARENESS

The DHSS Health Privacy team promotes public awareness of health privacy throughout NWT. The following resources were developed to inform residents about privacy rights:

- The DHSS website contains a dedicated space/tile for privacy. A website visitor can choose "privacy" as a filter to resource categories when searching privacy related documents, forms, posters and flyers. Examples of resources include but are not limited to:
  - Health Information Act Guide- https://www.hss.gov.nt.ca/sites/hss/files/hia-guide.pdf
  - Know your privacy rights- https://www.hss.gov.nt.ca/sites/hss/files/resources/know-your-privacy-rights.pdf
  - Notice of information collection, use and disclosure (Health Information Act) - https://www.hss.gov.nt.ca/en/services/protecting-your-privacy-health-and-social-services-system/notice-information-collection-use
  - Protecting your privacy within health information systems - https://www.hss.gov.nt.ca/sites/hss/files/resources/protecting-your-privacy-within-electronic-health-information-systems.pdf
  - Protecting your privacy in the health system - (available in many indigenous languages) https://www.hss.gov.nt.ca/sites/hss/files/hia-brochure.pdf
  - Request to access or correct you own personal health information- https://www.hss.gov.nt.ca/sites/hss/files/resources/request-access-correct-health-info-yours.pdf
  - Request to access or correct personal health information on someone's behalf- https://www.hss.gov.nt.ca/sites/hss/files/resources/request-access-correct-health-info-someone-behalf.pdf
- Many privacy materials are translated into NWT Official Languages and/or can be requested in other formats.
- Ministerial Directives are published on HSS website.
- Designated contact persons are appointed across HSS departments (DHSS and HSSAs) to manage privacy related issues, complaints, and investigations.
- Where the public has additional questions, they are encouraged to contact the Chief Health Privacy Officer via phone 867-767-9054 or email: HIA@gov.nt.ca

Ongoing public promotion efforts of HIA to residents through newspapers, website and social media advertisements inform NWT residents on how they can access their own PHI, and clients' rights to set consent conditions or review who has accessed their PHI.

1.4. ONGOING RESPONSIBILITIES

DHSS is committed to:

- Assessing privacy approaches and identifying potential vulnerabilities and opportunities for enhancements of the health privacy framework in NWT.
- Working effectively and collaboratively with HSSAs, physicians and pharmacists with their own businesses who are not employed by other custodians, the GNWT Office of the Chief Information Officer and NWT OIPC to maintain an effective privacy management program.
- Monitoring advancements in emerging technologies to ensure that the use of such technologies maximizes value for the HSS system while protecting NWT individuals' PHI and complying with applicable privacy legislation and best practices.

Part 2 – Review and Discussion of Health Information Act and Regulations

2.1. INTERPRETATION AND APPLICATION OF HIA

The *Health Information Act* consists of two pieces of legislation, (1) the Act and (2) the Regulations, which define terms used and assist with application and interpretation of the legislation. Section 1 of the HIA outlines a list of terms and provides guidance with interpretation. Definitions play an essential role in understanding the meaning of terms used throughout the HIA.

2.1.1. ADDING NEW TERMS INTO DEFINITIONS

Feedback collected from invested organizations since 2015 revealed some need to consider clarifying terms in future amendments such as:

- privacy breach
- 'need to know' versus 'circle of care'
- statistical versus anonymized information
- public health surveillance
- 'view' – add meaning to the term "use"
- secure use of PHI on mobile devices
- non-identifying information

DISCUSSION & FINDINGS

Clear definitions help ensure consistent application of the law and support transparency to allow those to whom the Act applies to better understand their obligations. Consistency and fairness are crucial for interpretation of any legislation. Making modifications to the meaning of terms, in order to clarify existing ambiguities, can improve interpretation but also lead to expanding or changing the scope of the Act itself.

Some of these terms are expanded on in greater detail later in this report (public health surveillance, secure use of PHI on mobile devices, and non-identifying information).

Existing definitions may be amended, where value added is substantial and has a beneficial impact on the interpretation of the HIA. When considering changing existing definitions or introducing a new term, a simple review can determine if there is a substantial value:

- The term 'privacy breach' as a concept is already explained in the HIA Part 4 (section 87) on the protection of PHI, where the Act identifies conditions that are not permitted, and what is or is not authorized. An explicit definition was developed and exists under the Ministerial Directive in the Privacy Breach Policy.

Is there a substantial value? No.
Conclusion: adding definition of 'privacy breach' is not required.

- The term 'need to know' as a principle does not appear in definitions. The phrase 'need to know' is not explicitly written into HIA, but the concept is included in section 28 which provides that a custodian shall not collect, use or disclose more PHI than is reasonably necessary for the purpose of the collection, use or disclosure. In healthcare settings the term 'circle of care' is more commonly used, to describe when a physician or other health care provider is accessing or disclosing a client's PHI under implied consent for a direct health care purpose because they are part of the patient's care team. However, acting on "circle of care" without any defined guardrails may lead to or cause confusion about the ability to access patient information, even when not currently involved in the patient's care. In 2024, Nova Scotia's Information and Privacy Commissioner issued guidance[2] and explained the weakness of 'circle of care' as a concept, and why the 'need to know' principle, which focuses on patient's healthcare needs, is more appropriate. Saskatchewan's Information and Privacy Commissioner in 2019 also found circle of care fails to protect patient's privacy.[3] In 2020, the NWT IPC at the time also recommended to cease using "circle of care" and replace it with "need to know.[4]

  Is there a substantial value to clarifying "need to know"? Yes.
  Conclusion: Solidifying a definition for the 'need to know' principle would support health information custodians and agents when they handle personal health information and strengthen client's trust.

- The term "use" means to handle the personal health information or apply it for a purpose, but not to collect or disclose the information. In training, DHSS emphasizes that seeing PHI, or 'viewing' it, is part of 'collection'. Ontario added 'to view information' into its definition of use, to be able to deal with snooping. Other jurisdictions have not followed Ontario's change. Snooping, or seeing PHI without authorization to do so, is still an unauthorized collection of PHI, which is already an offence in HIA.

  Is there a substantial value? No.
  Conclusion: changing the definition of 'use' to include "to view information" is not required.

CONCLUSION

Each submission from invested organizations on proposed changes to existing definitions or introducing new terms would benefit from completing an assessment from the 'value added' perspective and its substantiation when measuring beneficial impact on ongoing improvements of the HIA and its interpretation.

[2]https://oipc.novascotia.ca/sites/default/files/PHIA/PHIA%20Tools/2024%2001%2024%20Need-to-Know%20Instead%20of%20Circle%20of%20Care.pdf
[3]Saskatchewan Health Authority involving Dr. R (Re), 2019 CanLII 7172 (SK IPC), <https://canlii.ca/t/hxc81>, retrieved on 2025-09-03, at paragraph 28.
[4]Review Report 20-HIA-32, Northwest Territories Health and Social Services Authority (Re), 2020 NTIPC 41 (CanLII), <https://canlii.ca/t/jbpxp>, retrieved on 2025-09-18.

2.2. ROLES AND RESPONSIBILITIES

This Part of the HIA sets out four roles: Health Information Custodians, Agents, Contact Persons and Information Managers. These are defined as:

> "agent" except in [certain subsections of the legislation] means a person or organization listed in subsection 9(2) that is authorized by subsection 9(1) to act as an agent;
>
> "Contact person" means a contact person designated under subsection 12(1), or the health information custodian, if the custodian is a natural person and acts as their own contact person;
>
> "health information custodian" means
>
> a. the Department [the Department of Health and Social Services],
> b. a medical practitioner, other than a medical practitioner acting as an agent of a health information custodian,
> c. a pharmacist as defined in subsection 1(1) of the *Pharmacy Act*, other than a pharmacist acting as an agent of a health information custodian,
> d. a prescribed organization responsible under the *Hospital Insurance and Health and Social Services Administration Act* for the management, control and operation of one or more facilities from which health services are provided, or
> e. a prescribed person or class of persons, or a prescribed organization other than an organization prescribed as a health information custodian under paragraph (d);
>
> "information manager" means a person or organization that provides one or more of the following services for a health information custodian:
>
> a. The processing, storage, retrieval or disposal of personal health information,
> b. The transforming of personal health information, including the transforming of personal health information to create or produce non-identifying information,
> c. Information management services, information system services or information technology services.

Health information custodians must have an information management agreement with an information manager before using the information manager's services. The GNWT Technology Service Centre is an information manager for the DHSS and HSSAs.

An agent is a person or organization that acts for or on behalf of a health information custodian in respect of the powers, duties and functions of the custodian relating to collection, use, disclosure, management, retention or disposition of PHI under the HIA. This includes employees, students, volunteers, appointees, contractors, people in an agency relationship with the health information custodian as that term is understood in law, information managers, and any people or classes of people prescribed in the Regulations.

Health information custodians are responsible for ensuring agents only collect, use or disclose personal health information in accordance with their powers and the HIA.

Health information custodians have responsibilities to protect and manage the PHI of individuals in accordance with the HIA. Health information custodians are also responsible for ensuring agents only collect, use or disclose PHI in accordance with their powers and the HIA.

ROLE 1 - HEALTH INFORMATION CUSTODIANS

Sections 7-8 of HIA outline the details as follows:

- Persons Responsible

The Deputy Minister of the Department on behalf of the DHSS and people prescribed in the Regulations are health information custodians. In the Regulations the Chief Executive Officer of the Hay River Health and Social Services Authority; Northwest Territories Health and Social Services Authority; and Tłı̨chǫ Community Services Agency have been prescribed.

- Standards, policies and procedures

Health information custodians must put standards, policies and procedures in place to implement the HIA, including safeguards to protect the information.

ROLE 2 - AGENTS

Sections 9-11 of HIA outline the details as follows:

- Authorization of agents

Employees, students, volunteers, contractors, and information managers shall not collect, use, disclose, manage, retain or dispose of PHI during the performance of duties or functions for the health information custodian unless they have been authorized.

ROLE 3 - CONTACT PERSONS

Section 12 of HIA outlines the details as follows:

- Designated contact person

A health information custodian must have a contact person to receive complaints and respond to access requests for PHI.

ROLE 4 - INFORMATION MANAGERS AND INFORMATION MANAGEMENT AGREEMENTS

Section 13 of HIA outlines the details as follows:

- Information Management Agreement

A health information custodian can have more than one information manager and must have an information management agreement in place before using an information manager. The agreement must contain terms listed in the HIA.

The custodian can only disclose information to the information manager once the information management agreement is in place.

An agreement is not required if the information manager is the GNWT Technology Service Centre, or the Department for one of the Health and Social Services Authorities.

- Unauthorized actions

An information manager must not contravene the information management agreement in the collection, use, or disclosure of PHI.

2.2.1. ADDING OTHER HEALTH CARE PROFESSIONALS AS HEALTH INFORMATION CUSTODIANS

Staff feedback collected since 2015 indicated a desire to add as health information custodians other health care professionals, such as: paramedics /ambulance providers, chiropractors, optometrists, opticians, dentists, denturists, or midwives. This would be similar to the list of custodians in Alberta's health information legislation.

Feedback has also indicated that other "non-custodians" who hold personal health information on NWT residents should be considered, such as:

- Canadian Armed Forces
- Medical Director in charge of health clinics at correctional facilities or mining camps
- Long term care or supported living organizations

Feedback was received from the Information and Privacy Commissioner to consider what the benefit would be of adding additional health information custodians.

DISCUSSION & FINDINGS

1. Relevant Provisions under the HIA

Key sections relevant to this analysis include:

- HIA, Section 1: Health Information Custodian means the people listed.
- HIA, Section 7: The Deputy Minister of HSS and people prescribed in the Regulations are custodians.
- HIA, Section 9: Agents include: employees, students, volunteers, appointees, contractors, people in an agency relationship with the custodian as that term is understood in law, information managers, and any people or classes of people prescribed in the Regulations.
- HIA Regulations, section 1: The CEOs of the HSSAs are custodians.

2. Assessment of custodians

The list of custodians was not meant to be exclusive to the current four custodians for the future; it was meant as a starting point to cover the main 'players' in the NWT health system.

Having explanations of who is a custodian in a few places across the HIA has created confusion. This perhaps could be simplified to the following list:

- The Deputy Minister of the Department
- The Chief Executive Officer of an organization listed in the Regulations
- A medical practitioner who is not acting as an agent of another custodian
- A pharmacist who is not acting as an agent of another custodian

Medical Practitioner has a specific definition in the *Interpretation Act* and the *Medical Profession Act*. They are a medical doctor or physician.

Employees of DHSS and HSSAs are agents. Many of these employees are also registered health professionals, such as nurses or midwives. These health professionals may not need to be listed separately as custodians, because they already have roles as agents.

Two additional jobs have been suggested to be listed as custodians. These are:

- Psychologists not employed by the GNWT-- "private psychologists"
- Public Guardian

CONCLUSION

Additional health information custodians can be added as needed to the Regulations. Policy work is needed to determine which additional custodians should be added.

2.2.2. PRIVATE CUSTODIANS

We also received feedback that psychologists with private practices (not employed by the GNWT) should be considered to be added as custodians. We have received feedback that pharmacists and physicians with their own clinics, not employed by the GNWT, are not aware that they are custodians in accordance with HIA.

DISCUSSION & FINDINGS

1. Relevant Provisions under the HIA

A "private custodian" is any health information custodian who is not a public custodian. Key sections relevant to this analysis include:

- HIA, Section 1: Health Information Custodian means the people listed, including medical practitioners with their own clinics and pharmacists who are not agents of the GNWT.
- HIA, Section 1 Definition of "public custodian": means the Department of Health and Social Services, or a prescribed board (the HSSAs).
- HIA, Section 9: Agents include: employees, students, volunteers, appointees, contractors, people in an agency relationship with the custodian as that term is understood in law, information managers, and any people or classes of people prescribed in the Regulations.

2. Assessment of Private Custodians:

The DHSS and the three HSSAs are public custodians, along with their employees and contractors who are agents. The medical practitioners (physicians) and pharmacists who are not employed by the public custodians within the GNWT are private custodians. Private and public custodians have the same roles, duties, and responsibilities in HIA.

The lists of custodians in the HIA are not meant to be exhaustive. Psychologists with their own clinics/offices could be added as private custodians.

However, the feedback also indicates that some physicians and pharmacists do not know that the HIA applies to them. Notification to and training for the pharmacists not employed by hospitals and physicians that run their own clinics outside of government, and any other private custodians that get added, should be implemented.

CONCLUSION

The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution. Additional private health information custodians can be added as needed to the Regulations. More policy work is needed to determine if an exhaustive list of custodians is desired, and which private custodians should be added.

2.2.3. PUBLIC GUARDIAN

We received feedback that the Public Guardian should be considered for addition as a health information custodian.

DISCUSSION & FINDINGS

1. Relevant Provisions under the HIA

The Public Guardian is not currently mentioned in the HIA. Key sections relevant to this analysis include:

- HIA, Section 1: Health Information Custodian means the people listed.
- HIA, Section 7: The Deputy Minister of HSS and people prescribed in the Regulations are custodians.

2. Assessment of Public Guardian:

The Public Guardian is not mentioned in the HIA. The Public Guardian is a statutory position in the *Guardianship and Trusteeship Act*, section 58 of which is paramount to the HIA. The Public Guardian helps family members or close friends become legal guardians of adults over 18 years old who are unable to make decisions about their personal or health care. However, the Public Guardian is also employed by the DHSS and reports to the Deputy Minister[5]

The PHI collected and used by the Public Guardian is technically held within DHSS under the custodian, the Deputy Minister.

There is confusion between the independent role of the Public Guardian under the *Guardianship and Trusteeship Act* and the Public Guardian's responsibility as an agent of the Deputy Minister in HSS.

CONCLUSION

The issue lies not with the legislative framework of the HIA but with the position of the Public Guardian within the DHSS. Policy work is needed to determine whether amendments to the HIA or the *Guardianship and Trusteeship Act* would be most appropriate.

[5]https://www.hss.gov.nt.ca/en/services/office-public-guardian.[4]Review Report 20-HIA-32, Northwest Territories Health and Social Services Authority (Re), 2020 NTIPC 41 (CanLII), <https://canlii.ca/t/jbpxp>, retrieved on 2025-09-18.

2.3 CONSENT

Consent as a concept is a foundational pillar in health information privacy. Under HIA, consent is required when a health information custodian wants to collect, use, or disclose an individual's PHI, unless HIA specifically allows it without consent. The legislation describes what constitutes the provision of consent by an individual.

The consent in HIA is specific to making decisions about PHI collection, use and disclosure; it does not involve consent to health care treatment.

Consent is outlined in sections 14-24 of HIA:

- Interpretation: knowledgeable consent (Section 14)

Knowledgeable consent means patients know why and how their PHI will be collected, used, and shared. They are aware that they have the right not to share their information.

- Elements of consent (Section 15)

Valid consent must identify the patient and is given by that individual, or other person(s) authorized to act on behalf of the individual, where allowed under HIA.

There are four elements of consent. For consent to be valid, consent must be:

1. Consent of the individual.
2. Related to information. The consent must be specific to the purpose for which the information is being collected, used, or disclosed.
3. Knowledgeable. The individual must be made aware of their rights, including:
   - ✓ The right to refuse or withdraw consent at any time.
   - ✓ The right to limit or place conditions on how their information is used or shared.
4. Voluntary. The individual must give consent freely, without pressure or coercion.

- Consent: Express or Implied (Section 16)

Consent to collect, use, or disclose PHI can be express (written or verbal) or implied (without signature, reasonably inferred from the circumstances). Express consent is required in specific cases outlined in HIA.

- Implied Consent (Section 17)
- Information for health service: implied consent (Section 18)

A custodian may rely on implied consent if:

- ✓ The information is collected, used, or disclosed for providing or assisting in the provision of a health service.
- ✓ The individual has been informed of the purpose and has not objected.
- ✓ The information is shared among custodians involved in the individual's care.

- Form of Express Consent (Section 20)
  - ✓ Express consent may be written or verbal.
    - o Written consent must include the individual's name and signature, date of consent, purpose and scope of the consent.
    - o Verbal consent must be documented in writing by the custodian.

- Conditions and Instructions (Section 20(4))
- Definition: "condition" (Section 22)
  - ✓ Individuals may place conditions or instructions on their consent for future collection, use or disclosure.
  - ✓ Custodians must assess individual's consent condition, inform them of any implications (i.e. the condition may result in significant harm or is impractical), take reasonable steps to comply with the condition, and document the condition on their record.
  - ✓ Conditions placed on consent by an individual are not retroactive and do not take effect if they restrict the recording or sharing of information:
    - o Required by law (for example a requirement to notify the RCMP in the event of a gunshot wound).
    - o Required by established professional and institutional standards of practice – i.e. professional ethics and Accreditation Canada standards.
    - o Required by a prescription monitoring program.

  - ✓ Consent conditions remain valid:
    - o after the individual's death
    - o when the individual's chart is otherwise inactive
    - o when providing further health services to the individual, verifying eligibility of that individual for a health service, and when disclosing for continued care (s. 44(3))
    - o when disclosing information about the individual who is injured, ill or incapacitated to a contact person who has a close personal relationship with the individual or a potential substitute decision maker (s. 45(2))
    - o when disclosing PHI about the individual when a patient or resident in a health facility to another person who has a close personal relationship with the individual (s. 46(b), s. 47)
    - o when using patient information for internal management purposes such as developing policies, training employees, evaluations, planning and resource allocation (s. 19(2), 34(a), 43(3))
    - o in respect of research requests received by the DHSS/HSSAs

- in respect of data extract requests received by the DHSS/HSSAs
- until an individual or substitute decision maker:
  - makes changes to the current consent conditions or
  - revokes or withdraws the current consent conditions

- Withdrawal of Consent (Section 24)
  - ✓ Individuals may withdraw consent at any time, in whole or in part.
  - ✓ Withdrawal must be documented and does not apply retroactively.

- Exercise of rights by other persons (Section 25)- Substitute Decision Makers
  - ✓ A substitute decision-maker may act on behalf of an individual who needs another person to exercise their rights specifically related to the collection, use and sharing of their PHI.
  - ✓ People acting as substitute decision-maker may include:
    - A parent or guardian if the patient is under 19 and is not a mature minor
    - A patient's guardian, trustee or a legal representative
    - A person who holds the patient's power of attorney or the person named in a personal directive
    - Anyone authorized in writing by a patient who is mentally competent
    - A deceased patient's personal representative, estate executor, or spouse
    - A deceased patient's relative or an adult who had a close personal relationship with the patient
    - A deceased patient's substitute decision-maker identified in accordance with the *Human Tissue Donation Act*

- Duty of Substitute Decision-Maker (Section 26)
  - ✓ Must consider the individual's wishes, values and beliefs.
  - ✓ Must act honestly and in good faith.
  - ✓ Must not act beyond their legal authority.

2.3.1. FEEDBACK GATHERED

Three areas specific to consent received feedback and were explored based on existing challenges.

1. MATURE MINOR CONSENT WHEN ADDRESSING COMPLEX ISSUES (AGE INDICATION FOR MATURE MINOR)

Mature minors do not need a parent/guardian to act as a substitute decision maker. Mature minor is the concept where the custodian determines if a person (minor) has the capacity to understand their rights and make decisions about their PHI collection, use and disclosure.

FEEDBACK RECEIVED

Since the HIA came into force in 2015, there have been requests to make its own subsection or define "mature minor" in the definitions section of the HIA.

HSSAs requested *"The HIA should define a mature minor and also include exceptions to the exercise of the right under section 25. For instance, in the case of an emergency, or where not notifying the child's parent or guardian of the child's health status could endanger the child, parental right to access health record in certain circumstances should be provided. Amendment to specifically set an age range of 13 to 18 years for mature minors who can make decisions, with a focus on their maturity. It [is too] broad to say under 19 years of age."*

Office of the Chief Public Health Officer suggested *"Mature minors or alternative decision makers does need to be addressed somewhere within legislation especially when addressing complex issues such as immunization."*

DISCUSSION & FINDINGS

1. Applicable sections of HIA

In NWT within the HIA framework, a mature minor means a person under the age of 19 (the age of majority), who is mature enough to make their own decisions about what happens to their PHI and they understand the consequences of their decisions. This is in section 25(1)(b):

> *25. (1) Any right or power conferred on an individual by this Act, including any authority of an individual in respect of the collection, use or disclosure of personal health information about him or her, may be exercised,*
> *(a) if the individual has attained 19 years of age, by that individual;*
> *(b) if the individual has not attained 19 years of age, but understands the nature of the right or power and the consequences of exercising the right or power, by that individual; …*

If the health care provider (that is a custodian or agent), who is proposing to use or disclose the minor's information, does not believe (on reasonable grounds) that the minor understands the nature or consequences of the decision to collect, use or disclose their personal health information, a parent or guardian makes the decision.

2. Comparison of jurisdictions

The rules for mature minors are set out either in legislation or the common law and differs whether the decision is regarding personal health information or health care treatment.

HIA specifically does not set one age at which consent can be provided by the minor for dealing with their health information. It is instead based on an assessment of the individual's capacity to consent.

The majority of other provinces and territories health information legislation is the same as NWT, based on the person's capacity to consent with no set age to give consent. Quebec appears to be the only jurisdiction in Canada that provides a specific age for a minor's consent in their provincial health information legislation[6]. In Quebec the age for a minor to consent on their own is 14 years old or older.

Other NWT legislation, the *Child and Family Services Act*, the *Children's Law Act and Adoption Act,* include provisions that identify the possible involvement / consent of minors who are aged 12 or older.

This is separate from decisions for health care treatment. Mature minors decisions for treatment are set by common law. The common law provides that the right to make medical decisions varies with the minor's maturity, with more intense scrutiny of the minor's maturity depending upon the severity of the potential consequences of treatment or refusal (i.e., seriousness of treatment and long-term side effects). The health care provider must determine whether a minor is a mature minor based upon an assessment of the patient who is under the age of majority and follow their own discretion.

3. Application to Mature Minors in the HIA

Consent to health care treatment (medical decisions) is outside of the scope of HIA.

The feedback suggests that more work to provide clarity and assistance to custodians regarding mature minors is needed. While setting an age seems very appealing, there is not a consensus on one specific age, even in NWT legislation.

CONCLUSION

The HIA is aligned with common law in other jurisdictions in Canada, however other resources and training should be considered to assist custodians to guide assessment of minors' maturity.

2. THE CONSENT SECTION IS LONG AND COMPLEX.

DISCUSSION & FINDINGS

1. Relevant Provisions under HIA

Consent is outlined in ten sections of HIA (sections 14-24). As previously stated, consent is a fundamental pillar of HIA. This part of the HIA provides guidance for how consent is established, what it means, what types of consent exists, and how and when individuals can apply or withdraw their consent.

[6] *Act Respecting Health and Social Services Information*, https://www.legisquebec.gouv.qc.ca/en/document/cs/R-22.1

In line with conventions for drafting legislation, each sentence about the topic of consent is given its own section. To convey the complex topic of consent ten sections have been used.

2. Comparative Jurisdictional Review

When reviewing health legislation from other Canadian jurisdictions' consent provisions range from 5 to 15 sections long, with varying levels of detail.

CONCLUSION

The length of the consent part is in line with other Canadian jurisdictions. Policy work should be done to see if these sections of the HIA can meaningfully be simplified.

3. SOME HIA PROVISIONS CANNOT BE IMPLEMENTED WITH EXISTING RESOURCES.

Office of the Information and Privacy Commissioner raised in one Review report the following: *"There is no ability within the EMR to implement the provisions in sections 22-23 that allow individuals to place conditions on their consent. The Client Conditions Policy is an attempt to manage this but does not address the technical inability to remove an employee's access to an individual's record. Our office recently addressed this in 2025 NTIPC 84."*

DISCUSSION & FINDINGS

HIA provisions empower individuals to exercise greater control over their PHI in the future while still balancing the operational and legal responsibilities of the custodians.

Some provisions (HIA Sections 22-23) present a challenge and cannot be fully enabled within the designated e-health information systems currently in use by DHSS and HSSAs due to technical limitations of the systems. The gap between legislative requirements and existing technical capabilities is a challenge for privacy compliance. DHSS is exploring options for system enhancements in the future. One of the interim approaches that HSSAs follow is manually documenting consent conditions and auditing for compliance.

When a client places a consent condition on the collection, use or disclosure of their PHI, it can inadvertently hinder the effectiveness of their care depending on the nature of the restriction. While clients have the right to control their information, certain conditions may unintentionally compromise safety, continuity, or quality of care. Any consent conditions need to be clearly explained to the NWT resident by the custodian to ensure they are understood, as well as any limitations in the ability to apply the condition in a designated eHealth system.

CONCLUSION

Amending the HIA will not solve the use of consent conditions in a particular eHealth system. Funding by the GNWT for system enhancement is outside of the scope of legislation.

2.4. COLLECTION, USE, DISCLOSURE AND PROTECTION OF PERSONAL HEALTH INFORMATION

HIA defines collection, use, and disclosure of health information:

> "collect", in relation to information, means to acquire, gather, obtain or receive information
>
> "use", in relation to information, means to handle, deal with or apply information for a purpose, including to reproduce or transform it, but does not mean to collect or disclose information
>
> "disclose", in relation to information, means to release information, or make information available in any manner, including verbally or visually, to a person or organization

Health information custodians are limited in how they collect, use, and disclose PHI to ensure privacy and confidentiality. They may only collect information that is necessary for lawful and specific purposes, such as providing health care. They can use the information solely for those intended purposes, such as treatment or health system planning, and cannot repurpose it without proper authorization. Disclosure of information, including sharing it with other individuals or organizations, is strictly controlled and typically requires consent or legal authority. Each of these actions, collection, use, and disclosure, have distinct definitions and boundaries that custodians must follow under HIA.

Collection of PHI is outlined in sections 27-33 of HIA:

- General Compliance (Section 27)

Health information custodians must comply with the HIA and regulations when collecting, using, or disclosing personal health information.

- Limiting Identifiable Information (Section 28)

Health information custodians must use non-identifying information if it is sufficient. They must not collect, use, or disclose more PHI than necessary, unless required by law.

- Lawful Collection (Section 29)

PHI can only be collected by a health information custodian if:

- ✓ The individual consents and the purpose is lawful.
- ✓ Collection is permitted or required by law.
- ✓ Another law allows disclosure to the custodian without consent.

- Collection from Other Sources (Section 30)

Custodians may collect PHI from sources other than the individual if:

- ✓ The individual consents.
- ✓ It's from a health service provider for care purposes.
- ✓ It's not practical to get it from the individual.
- ✓ Collecting directly could harm the individual or the data's accuracy.
- ✓ It's necessary for eligibility verification, genetic history, legal reasons, or approved research.

- Duty to Inform (Section 31)

When collecting PHI, health information custodians must inform individuals (or substitute decision makers) about:

- ✓ The legal authority for collection.
- ✓ Intended uses and potential disclosures.
- ✓ Rights related to consent.
- ✓ Who may receive the information without consent.
- ✓ A contact person for questions.

- Use of Personal Health Numbers (Section 32)

Individuals or health information custodians can collect or use a personal health number (health care card number) for the following:

- ✓ It's disclosed by a custodian for a valid purpose.
- ✓ It's required by law or regulation.
- ✓ The individual must be informed of the legal authority behind the request.

- Use of Recording Devices (Section 33)

Health information custodians must notify individuals if PHI will be collected using hidden or non-obvious recording devices.

Use of PHI is outlined in sections 34-37 of HIA:

- Consent and Lawful Use (Section 34)

A health information custodian may only use PHI if:

- ✓ The individual consents and the use is for a lawful purpose.
- ✓ The use is permitted or required by law (territorial, provincial or federal).
- ✓ The use aligns with a purpose for which disclosure to the custodian was legally allowed without express consent.

- Permitted Uses Without Additional Consent (Section 35)

Health information custodians may use PHI for various operational and care-related purposes, including:

- ✓ Providing health services or for the purpose it was originally collected.
- ✓ Eligibility assessments for programs or services.
- ✓ Internal management, such as:
  - o Planning, policy development
  - o Quality improvement and evaluations
  - o Billing and legal or risk management
  - o Training staff
- ✓ Facility inspections or investigations.
- ✓ Research that meets legal conditions.
- ✓ Seeking consent, using only name and contact info.
- ✓ Creating de-identified data.
- ✓ Legal compliance (e.g. court orders).
- ✓ Education of health service providers.

- Data Handling and Transformation (Section 36)

Health information custodians may:

- ✓ Transform PHI into non-identifying information, such as de-identifying or encoding it.
- ✓ Combine or compare PHI from multiple electronic sources, as long as the use is legally permitted.

- Additional Uses for Public Custodians (Section 37)

Public custodians may also use PHI for:

- ✓ Health system management, including service planning and evaluation.
- ✓ Public health activities, such as surveillance and promotion.
- ✓ Enforcing compliance with HIA and its regulations.

Disclosure of PHI is outlined in sections 38-66 of HIA:

- General Conditions for Disclosure (Section 38)

Health information custodians may disclose PHI about an individual if:

- ✓ The individual has provided explicit consent, and the disclosure is necessary for a lawful purpose.
- ✓ The disclosure is permitted or required by HIA, another Act, or Canadian law or regulation.

- Verification Before Disclosure (Section 39)

Before disclosing PHI, health information custodians must take reasonable steps to verify that the recipient is authorized to collect the information and the intended recipient.

- Definition of "Recipient" (Section 40)

A "recipient" is defined as a person or organization to whom PHI is disclosed, excluding:

- ✓ Other health information custodians.
- ✓ The individual to whom the information pertains.

Recipients may only use or disclose PHI for the original purpose the custodian was authorized to disclose it for, or to fulfill a legal obligation.

- Disclosures Without Consent (Sections 41- 66)

Health information custodians may disclose PHI without express consent under specific circumstances, including:

- ✓ For providing access to an individual's own health information.
- ✓ To another custodian for purposes related to s.35 and s.37.
- ✓ To the Information and Privacy Commissioner for exercise of powers or duties.
- ✓ To health service providers for the purpose of providing or assisting in the provision of health services.
- ✓ To a person responsible for providing continuing care or treatment to an individual.
- ✓ For contacting a person in a close personal relationship with the individual if the individual is unable to provide consent due to injury, illness, or incapacity.
- ✓ For informing relatives or close associates of the death of an individual and related health services provided.
- ✓ For determining or verifying eligibility for health services or benefits.
- ✓ For purposes related to legal proceedings, such as complying with court orders or legal processes.
- ✓ To detect or prevent fraud, limit abuse, or prevent the commission of an offense under an enactment.
- ✓ For law enforcement purposes when required.
- ✓ For arrangement of health services for individuals in detention facilities.
- ✓ To prevent or reduce an imminent threat to health or safety.
- ✓ When transferring records to a successor custodian.
- ✓ For audit or legal services.
- ✓ For developing, managing, monitoring or evaluation health systems or programs to other government bodies.
- ✓ For compiling and analyzing statistical information.
- ✓ For reviewing complaints by an individual about health services provided by a public custodian.
- ✓ To electronic health information systems for delivery of health services.

- ✓ To maintain a health registry.
- ✓ For prescription monitoring program under *Pharmacy Act.*
- ✓ To government health agencies for public health purposes if required by law.

FEEDBACK GATHERED

2.4.1. USE OF MOBILE DEVICES TO DISCLOSE IMAGES FOR CONSULTATION

In clinical practice, physicians in NWT at times take photographs of a patient's condition (e.g., visible injuries, dermatological concerns) using a personal or work-issued mobile device and transmit these images to other healthcare professionals for the purposes of diagnosis, treatment, or consultation. This practice, while potentially beneficial for timely and effective patient care, raises concerns regarding compliance with HIA, particularly with respect to disclosure, consent, privacy, and security.

DISCUSSION & FINDINGS

1. Relevant Provisions under HIA

The HIA governs how personal health information (PHI) may be collected, used, and disclosed by health information custodians. Key sections relevant to this analysis include:

- HIA, Section 44: Custodians may disclose PHI under implied consent for the purpose of providing or assisting in the provision of health care to the individual.
- HIA, Section 85: Requires health information custodians to protect PHI by making reasonable administrative, technical, and physical safeguards, including ensuring agents are properly trained in duties and responsibilities under the HIA.
- HIA Regulations, Section 13: Requires custodians to establish policies and procedures to prevent unauthorized access, use, or disclosure of PHI.

2. Assessment of the Practice: Taking and Sending Photos for Consultation

a. Permissible Disclosure for Care (Section 44)

Taking and sending photos for consultation aligns with s.44, as it qualifies as a disclosure to a person responsible for providing continuing care or treatment. Thus, it can be permissible without additional patient consent, provided it is reasonably necessary for care and in line with professional standards. However, express consent from the patient for this type of disclosure is preferable.

b. Training and Policies (Section 85)

These practices highlight the need for physicians to be correctly trained in secure handling of PHI and ensure that processes are in place to appropriately transmit and save the personal information collected. Section 85 mandates that custodians maintain administrative, technical and physical safeguards for the protection of PHI. One of these administrative safeguards is ensuring agents complete privacy training established under the Ministerial Directive – Privacy Standards, Policies and Procedures. If inappropriate or ad-hoc methods (e.g., WhatsApp, unencrypted texting) are used, it may reflect a training or policy gap rather than a legislative one.

c. Security and Safeguards (HIA Regulations, Section 13)

The concern lies not in the disclosure itself, but in how it is done. If physicians use personal devices without proper encryption, secure transmission, or organizational oversight, this could violate s.13(c) and (f), which requires health information custodians to encrypt and protect PHI stored electronically, and protect PHI stored and transported on removable media. Examples of risk include:

- Storing images on unencrypted phones.
- Sending images over unsecured messaging apps (e.g., SMS, personal email).
- Lack of audit trails for access and transmission.

CONCLUSION

Legislation is sufficient – training and policy are the issue. There is no need to amend the HIA to address this specific practice. The HIA already:

- Permits disclosures for care.
- Requires safeguards for PHI.
- Imposes training and policy obligations on health information custodians.

Instead, improved organizational standard operating procedures and training on acceptable transmission of media should be implemented to ensure compliance. Key recommendations include:

- Training programs for physicians on acceptable technologies and secure communication.
- Clear policies and operating procedures developed by HSSAs on when and how mobile devices can be used.
- Provision of secure apps or tools (e.g., secure messaging platforms approved by the health information custodian).
- Auditing and monitoring practices to ensure compliance.

The current HIA adequately addresses the use and disclosure of patient photographs for consultation purposes. The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution.

2.4.2. CANCER SURVEILLANCE PROGRAM

A territorial cancer surveillance program offered in the NWT aims to enhance early detection by identifying and directly contacting individuals at average risk (i.e., asymptomatic, without high-risk history) to encourage participation in screening programs (e.g., colorectal, cervical, breast cancer). This involves accessing and using personal health information PHI to:

1. Determine eligibility based on age, sex, or medical history.
2. Directly contact patients by mail with a collection kit, and lab requisition.

This raises questions about the legality of collecting, using, and disclosing PHI for these purposes under the current legislative framework.

DISCUSSION & FINDINGS

1. Collection and Use of PHI under the HIA

a. Section 30 (Collection from Other Source):

Health information custodians may collect PHI without the consent of the individual if the information is necessary and being collected for the purpose of determining if someone qualifies for participation in a health program or to verify ongoing eligibility for a health service or product. The use of the phrases *"necessary"* and *"being collected for the purpose of"* signals a narrow and specific collection authority. In this context, the HIA does not provide a clear path for programs that consider using specific eligibility parameters, such as age or gender, in setting a plan for prevention or screening activities (for example Cancer Surveillance Program). Any population-based surveillance or outreach is linked to the need for collecting PHI to identify individuals who may be eligible for a program. Section 30 of the HIA is not clear about what limitations may exist for the use of existing health data to automatically enroll or invite individuals to participate in the program.

b. Section 35 (Use of PHI by Health information custodians):

Health information custodians may use PHI for the purpose for which it was collected, and for functions reasonably necessary for carrying out that purpose. Using PHI to contact patients for population health screening may not be considered a consistent purpose unless it is directly tied to the patient's original care encounter.
While collection and use of PHI for individual care is allowed, using PHI to proactively identify average-risk individuals outside of clinical interaction likely exceeds what is currently authorized without consent.

2. Disclosure of PHI for Screening Outreach

Section 48 (Disclosure without Consent):

Section 48 disclosure provisions mirror Section 30, in that health information custodians may disclose PHI without the consent of the individual if the information is necessary and being collected for the purpose of determining if someone qualifies for participation in a health program or to verify ongoing eligibility for a health service or product. Once again, the condition is the use of the phrases *"necessary"* and *"being collected for the purpose of".*

There is currently no explicit provision in the HIA or its regulations allowing disclosure of PHI for the purpose of direct mailing average-risk individuals without consent as part of a proactive screening initiative.

3. Privacy Implications and Risk

Direct mailing for cancer screening may significantly improve participation and early detection. However, without a clear legislative basis:

- Such disclosure risks violating privacy rights.
- Individuals may be unaware their information is being used this way.
- There is a lack of clarity for custodians about permissible actions, increasing legal and reputational risk.

CONCLUSION

While the intent of the Territorial Cancer Surveillance program is aligned with preventative health objectives, the current provisions of the HIA and Regulations do not clearly permit the collection, use and disclosure of PHI for the purpose of directly contacting average-risk individuals for cancer screening.

Consideration could be given to amend the HIA Regulations to include a specific provision authorizing the disclosure of PHI for the purposes of organized population-based screening programs. This could be modeled after language used in other jurisdictions (e.g., Alberta's Cancer Registry Regulations or Ontario's regulations under the *Personal Health Information Protection Act*, 2004), and should include:

- Definition of screening programs as a permitted purpose.
- Designation of the cancer surveillance program as a prescribed organization or authorized recipient.
- Conditions for privacy safeguards and oversight.

2.4.3. DISCLOSURE OF PHI FOR JOINT GUARDIANSHIP AND TRUSTEESHIP APPLICATIONS

In the NWT, individuals may apply for guardianship (to make personal or health decisions) and/or trusteeship (to manage financial affairs) for an adult who lacks capacity. These applications are often submitted jointly. Although the offices work closely together, the Office of the Public Guardian (OPG) resides with the DHSS and is subject to the HIA, and the Office of the Public Trustee (OPT) resides with the Department of Justice and HIA does not apply.

Under the current process for guardianship or trusteeship orders, all intake information is received and processed by the OPG who does not share client applicant information with the OPT until they identify a need for an application for trusteeship. This was identified by the OPT/OPG office as possibly hindering the joint application process.

Disclosure of PHI by the OPG must comply with:

- Section 50 of the *Health Information Act* (HIA) – governing disclosure by custodians.
- Section 58 of the *Guardianship and Trusteeship Act* (GTA) – governing release of health information for guardianship/trusteeship proceedings.

DISCUSSION & FINDINGS

1. Legislative Analysis

Section 50 of the *Health Information Act* (HIA) – Disclosure by custodians

Section 50 of the HIA allows custodians to disclose PHI without consent only as permitted by the Act, such as:

- With authorization from another Act,
- Under a court order,
- To a legal representative or substitute decision-maker (if already appointed).

In joint applications, the applicant has not yet been appointed a guardian or trustee. As such, the OPG is not authorized under the HIA to disclose PHI to the OPT, unless another statute (like the GTA) explicitly permits it. Additionally, the OPG is considered an agent, not a custodian under the HIA.

Section 58(4) of the *Guardianship and Trusteeship Act (GTA) – Authority to Disclose Information for Proceedings*
Section 58(4) of the GTA authorizes disclosure of PHI to the court for the purpose of determining a person's capacity without an individual's consent and applies notwithstanding the HIA.

Limitations of s.58(4) GTA:

- The provisions enable disclosure of "information provided in a report" but there is some ambiguity if this is to be interpreted as when the report has been completed or enables disclosure of intake information in support of the report.

2. Jurisdictional Context and Comparators

Other jurisdictions (e.g., Alberta, Ontario) have created specific provisions in their guardianship or health information laws to support:

- Limited disclosures to individuals initiating a substitute decision-making process,
- Clear legal authority for capacity assessments to be shared for application purposes,
- Privacy safeguards such as "minimum necessary" disclosures or secure communication channels.

CONCLUSION

Primary Recommendation: Amend the Guardianship and Trusteeship Act (GTA)

Amending the GTA is the preferred and targeted solution because:

- The need for PHI arises within the guardianship/trusteeship context, not the general health system.
- The GTA already governs the process and roles of parties involved.
- A focused amendment would provide legal clarity to the PGO, health professionals, legal counsel, and applicants.

Secondary Consideration: Amend the *Health Information Act* (HIA)

While not strictly necessary, limited amendment to the HIA could be considered to:

- Create a permissive clause that allows disclosure of PHI in specific legal proceedings (e.g., guardianship applications) even before a decision-maker is appointed.
- Ensure the HIA complements rather than restricts the GTA.

The current legislative framework creates practical and legal challenges in preparing joint guardianship and trusteeship applications due to limits on the disclosure of personal health information.
Amending the GTA would more directly and effectively address the issue of PHI disclosure in this context, ensuring timely and lawful access to necessary information. However, consideration could also be given to amending the HIA to permit limited, purpose-specific disclosure when doing so would benefit the client.

2.4.4. DISCLOSURE OF PHI TO THE NWT HEALTH AND SOCIAL SERVICES LEADERSHIP COUNCIL

The NWT Health and Social Services Leadership Council, established under section 10.1 of the *Hospital Insurance and Health and Social Services Administration Act* (HIHSSA), plays an oversight and strategic advisory role in the HSS. It may be involved in reviewing service delivery performance, providing input on system improvements, and advising on policies and priorities.

As part of its work, the Council may request access to data or reports related to health outcomes, service access, or population needs. This raises the question of whether personal health information (PHI) can be disclosed to the Council under the HIA.

DISCUSSION & FINDINGS

1. Legal Framework – *Health Information Act* (NWT)
The HIA governs how health information custodians (such as HSSAs) collect, use, and disclose PHI. The default rule is that PHI cannot be disclosed without the individual's consent, unless a specific exception applies.

Key sections relevant to this analysis:

- Section 30: Outlines when PHI may be collected from another source.
- Section 35: PHI may only be used for the purposes for which it was collected or for a consistent purpose.
- Section 41- 66: Disclosure without consent is permitted only in specific circumstances (e.g., for providing care, complying with another law, or system planning where allowed).
- Section 85: Requires custodians to establish policies and safeguards to prevent unauthorized disclosure.
- Definition of "non-identifying information[7]": refers to PHI that cannot be reasonably used to determine an individual's identity or lead to re-identification.

2. NWT Leadership Council

a. Is the Leadership Council a "Health Information Custodian" or Authorized Recipient?

The Leadership Council is not a health information custodian under the HIA and is not listed as a prescribed organization under the HIA or HIA regulations for the purposes of receiving PHI without consent. The Council does not have legal authority under the HIA to receive identifiable PHI without individual consent or a specific legislative mandate.
b. Is Disclosure of Identifiable PHI Justified?

[7] Ministerial Directive, Privacy Standards, Policies and Procedures. Health and Social Services De-identification Policy, 2017.

While the Leadership Council may request data to inform its advisory functions, it does not provide direct care, make individual-level decisions, or require identifiable information to fulfill its mandate.

- Its functions relate to system-level oversight, planning, and evaluation.
- Identifiable PHI is not necessary for these purposes.

Conclusion: Disclosure of identifiable PHI to the Leadership Council is not permitted under the HIA, as it is not necessary and there is no specific legal authority allowing it.

c. Is De-Identified Information Sufficient?

The NWT Leadership Council's work can be fully supported with de-identified or aggregate data, including:

- Trends in service utilization,
- Health outcomes by health region or population,
- Wait times, provider distribution, and resource use.

Under the HIA, de-identified information is not considered PHI and is not subject to the same restrictions on use or disclosure.

HSSAs can provide the NWT Health and Social Services Leadership Council with de-identified summaries, dashboards, and reports that support its role without breaching privacy.

CONCLUSION

Under the HIA, there is no authority for health information custodians to disclose identifiable PHI to the NWT Health and Social Services Leadership Council without consent. However, the Council's oversight and advisory role can be fully supported with de-identified information.

2.4.5. DISCLOSURE OF PHI TO OTHER GOVERNMENT BODIES

Other government departments such as the Department of Education, Culture and Employment (ECE) and Executive and Indigenous Affairs (EIA) administer a range of services that may intersect with health-related information needs, such as:

- Student support services in schools (e.g., learning accommodations, mental health counselling),
- Income support programs, including payment for room and board for long-term care, and
- Integrated service delivery.

These services often rely on or benefit from health-related information. However, the question arises whether custodians are permitted to disclose PHI to other government bodies under the current HIA framework.

DISCUSSION & FINDINGS

1. Legal Framework – Health Information Act (NWT)

Under the HIA, health information custodians may only disclose PHI without the individual's consent in specific, limited situations.

Key sections include:

Section 1 (Definitions) – Health information custodians include the DHSS, HSSAs, and private pharmacists and medical practitioners, but not education or other public bodies or agencies.

Section 41-66 (Disclosure without consent) – Allows disclosure only in defined circumstances, such as:

- For providing health care,
- To comply with other legislation,
- For health system management to prescribed entities.

Section 85 – Requires custodians to safeguard PHI and ensure its disclosure only as permitted.

Unless another Act or regulation explicitly authorizes it, health information custodians cannot disclose PHI to a department like ECE or EIA for education, income support, or integrated service delivery without the individual's consent.

2. Disclosure to Other Government Bodies Is Not Authorized Under the Current HIA

ECE or EIA are not a prescribed organization under the HIA, nor are they listed as an organization to which PHI may be disclosed without consent. The Departments also don't meet the definition of a health information custodian.

Even when acting in coordination with health service providers (e.g., payment for long-term care or education supports), ECE or EIA do not have legal authority under the HIA to receive identifiable PHI without the express consent of the individual (or their substitute decision-maker, if applicable).

Under current legislation, health information custodians may not disclose PHI to ECE or EIA without consent. There is no legal authority in the HIA or its regulations to support such disclosures.

3. Comparative Review – Other Jurisdictions

Several Canadian jurisdictions have amended legislation or created regulatory frameworks to enable interdepartmental information sharing in limited, controlled ways for integrated service delivery.

Examples include:

Ontario – *Personal Health Information Protection Act and Child, Youth and Family Services Act:*

- Enables specific health and education/social services agencies to share PHI without consent when part of a "multi-disciplinary team" delivering coordinated services to a child or youth.
- Applies in cases where failure to share could harm the individual or delay critical support.

Alberta – *Health Information Act and Freedom of Information and Protection Act:*

- Requires express consent for most disclosures to non-health bodies like education or income support.
- However, specific information-sharing agreements can be developed under cross-ministry frameworks.

Other jurisdictions allow disclosure of PHI to education or income support ministries only when explicitly authorized by law or through narrowly defined inter-ministerial frameworks, often with safeguards such as privacy impact assessments, role-based access, and minimum necessary use.

5. Policy Implications and Considerations for the NWT

If the NWT is considering enabling appropriate PHI disclosure to another government body in specific circumstances (e.g., to support students with complex needs or integrated service delivery), it must:

1. Conduct policy engagement regarding amending the HIA or its regulations to:
    - Identify the government body (or specific programs) as a prescribed organization to receive PHI,
    - Limit the scope to defined purposes (e.g., integrated service delivery, income support determinations),
    - Require appropriate privacy safeguards.

2. Develop interdepartmental information-sharing frameworks, including:
    - Consent protocols or waiver conditions,
    - Oversight and data minimization requirements,
    - Privacy impact assessments.

CONCLUSION

Under the current HIA, health information custodians are not authorized to disclose identifiable PHI to ECE or EIA for schools, income support, or integrated service delivery purposes without the individual's consent.

More policy work is needed to identify the scope of policy or legislative amendments to appropriately target such a disclosure for these purposes. Other Canadian jurisdictions have addressed this issue through targeted amendments and multi-agency frameworks that balance service integration with privacy protections.

2.4.6. JURISDICTIONAL CLARIFICATION OF SECTION 50(B) OF HIA

Section 50 of the HIA sets out the general rule that health information custodians must not disclose PHI unless permitted by the Act. Section 50(b) is one of the exceptions, allowing disclosure without consent where required to comply with legal instruments, such as:

- A summons, subpoena, or warrant;
- A demand or order issued by a court, person, or organization with the authority to compel production;
- A rule of court governing the production of information.

This provision ensures custodians can respond to lawful obligations to provide information for judicial or quasi-judicial proceedings.

DISCUSSION & FINDINGS

1. Current Wording of Section 50(b)

A health information custodian may disclose personal health information about an individual:

> (b) for the purposes of complying with
> *(i) a summons, subpoena or warrant issued or a demand or order made by a court, person or organization that has the authority to compel the production of information, or*
> *(ii) a rule of court that relates to the production of information;*

While this provision appears broad and functional, it does not explicitly restrict authority to NWT court or entities. It lacks explicit reference to jurisdiction, leaving open the question of whether orders issued outside the NWT (e.g., from another province or federal court) authorize disclosure under this section.

2. Implications of Ambiguity

Because Section 50(b) does not clarify jurisdiction, custodians may be unsure whether:

- They must comply with subpoenas or orders from other provinces;
- They can disclose PHI without consent in response to a legal order from outside NWT;
- They risk breaching the HIA if they disclose PHI under an invalid order.

Without a jurisdictional qualifier, there is a risk of:

- Unlawful disclosure of health information;
- Inconsistent interpretation across custodians;
- Erosion of trust in how personal health information is protected.

3. Comparative Jurisdictional Review

Section 50(b) is currently worded the same as the section in Saskatchewan's legislation, and similarly to those in Prince Edward Island and Newfoundland and Labrador.

Ontario – *Personal Health Information Protection Act* (PHIPA):

- PHIPA permits disclosure in response to a court order or subpoena, but in practice, only Ontario court orders are enforceable unless recognized by an Ontario court.
- The wording is more concise but interpreted narrowly under Ontario procedural law.

Manitoba – *Personal Health Information Act* (PHIA):

- Disclosure is required to comply with a subpoena, warrant or order issued or made by a court having "jurisdiction to compel production".
- Jurisdiction to compel implicitly requires the issuing authority to have legal jurisdiction in Manitoba and therefore must be reviewed and endorsed by a Manitoba court to have effect.

Alberta – *Health Information Act* (HIA):

- Alberta's HIA only recognizes a subpoena, warrant, or order issued or made by a court "having jurisdiction in Alberta". This is a clear jurisdictional qualifier.
- Additionally, custodians are guided by Alberta's Rules of Court, which require domestication of foreign (out-of-province) orders before compliance.

The provincial legislation described above implicitly or explicitly limits disclosure to legal instruments that are enforceable within their own jurisdiction. Alberta provides a useful model for clarity, while others rely on civil procedure rules and legal interpretation to limit disclosure based on jurisdiction.

4. Recommendations and Legislative Options

Primary Recommendation: Amend Section 50(b) to Clarify Jurisdiction

Given the potential for misinterpretation and the practice in other provinces, Section 50(b) would benefit from a targeted amendment in the future to clearly state that only subpoenas, warrants, or court orders issued or enforceable within NWT jurisdiction permit disclosure.

- Aligns with Alberta's approach;
- Provides clear direction to custodians;
- Enhances privacy protection by ensuring only local or legally enforceable instruments apply;
- Reduces legal risk and administrative confusion.

Secondary Recommendation: Operational Policy

In the absence of immediate legislative change, custodians can implement a standard operating procedure (SOP) or amend the existing Ministerial Directive – Privacy Standards, Policies and Procedures to verify the validity of subpoenas, warrants, and court orders before disclosing PHI.

This should include:

- A requirement to confirm the issuing body's jurisdictional authority over the custodian;
- A step to consult legal counsel if the subpoena originates outside the NWT;
- A policy to decline or defer disclosure unless the legal instrument is:
  - clearly enforceable in NWT, or
  - recognized by an NWT court.

This approach empowers custodians to make consistent, legally sound decisions about when to disclose PHI under Section 50(b) and helps mitigate risk in the absence of legislative clarity.

CONCLUSION

Section 50(b) of the HIA would benefit from a legislative amendment in the future to explicitly state that only subpoenas, warrants, and legal orders enforceable within NWT jurisdiction authorize the disclosure of PHI without consent. This would align the HIA with best practices in jurisdictions like Alberta and provide certainty to custodians.

As a secondary option, in the absence of an amendment, custodians should adopt a formal policy or SOP requiring verification of jurisdictional validity before disclosing PHI in response to legal instruments. This would help ensure lawful disclosure, support consistent decision-making, and uphold the privacy principles underlying the HIA.

2.4.7. MANAGING PUBLIC HEALTH OUTBREAKS AND DUTY OF CARE

During public health outbreaks, such as measles or tuberculosis, effective response requires access to PHI, including diagnosis, contact tracing, and immunization status. These actions are critical to:

- enable contact tracing,
- protect unvaccinated individuals,
- inform treatment decisions, and
- prevent further transmission.

In the NWT, this need is met through provisions in the HIA and the Public Health Act (PHA). Physicians also play a critical role through their duty of care to patients.

DISCUSSION & FINDINGS

1. Legislative Framework in NWT

Health Information Act (HIA)

- Section 41-66 (Disclosure without consent) – Allows disclosure only in defined circumstances.
- Section 66: Allows health information custodians to disclose PHI without consent if required by another enactment, such as the PHA.

Public Health Act (PHA)

- Section 22: For example physicians and labs must report notifiable diseases, such as measles, to the Chief Public Health Officer (CPHO).
- Section 35- 38: The CPHO may collect, use, and disclose PHI without consent to investigate or manage an outbreak, public health surveillance, or support immunization programs

These provisions provide a comprehensive legal pathway for sharing necessary health information during an outbreak.

2. Physician Access and Duty of Care

Physicians employed by HSSAs are agents under the HIA and may access PHI, including immunization records, of patients in their care panels. This is not considered disclosure but a use of information as part of providing direct health care.

In addition, physicians have a duty of care, which:

- Requires them to act in their patients' best interests,
- Includes taking reasonable steps to prevent foreseeable harm,
- Supports proactive review of immunization status during a public health risk.

Physicians are both legally and ethically supported in reviewing and using patient immunization data to protect patients under their care, particularly in outbreak scenarios.

3. How Does NWT Compare to Other Provinces and Territories?

NWT legislation is consistent with national public health and privacy legislation. All Canadian jurisdictions authorize:

- disclosure of PHI to public health authorities without consent for outbreak management, and
- physician access to immunization data for patients under their care.

4. Summary of Legal, Clinical, and Ethical Foundations

Scenario	Legal basis	Express patient consent required?	Supported by Duty of Care?
Public health accessing immunization and case data	PHA (s.36, s.38), via HIA s.66	**No**	**Yes**
Reporting notifiable diseases	PHA s.22, via HIA s.66	**No**	**Yes**
Physicians reviewing immunization records of patients under their care	Authorized use under HIA	**No**	**Yes**
Physicians advising patients or initiating catch-up vaccination for patients in their care panel	Standard of care	**No**	**Yes**

CONCLUSION

The HIA and PHA in the NWT provide a legally sufficient and nationally aligned framework for the disclosure and use of PHI during public health outbreaks such as measles.

Disclosure to public health officials is authorized without consent under Section 66 of the HIA, referencing the clear authority granted under the PHA. Furthermore, physicians may access the immunization status of their patients as part of providing care and are ethically obligated, under the duty of care, to use that information to protect patients' health.

There is no demonstrated requirement to amend the HIA to support these functions. The existing legislative framework aligns with other Canadian jurisdictions and adequately supports both public health surveillance and clinical responsibilities.

2.4.8. PUBLIC HEALTH SURVEILLANCE

Under the current legal framework in the Northwest Territories, the Chief Public Health Officer (CPHO) lawfully receives PHI related to notifiable chronic diseases through provisions in both the HIA and the PHA. This information is used to support public health surveillance activities, including the monitoring of disease prevalence, identifying trends, informing policy development, guiding prevention strategies, health promotion, and development of public health programs. Chronic disease data collected by the CPHO is essential for understanding long-term population health outcomes in the NWT and supporting evidence-based decision-making across health systems.

DISCUSSION & FINDINGS

1. Legal Authority for the CPHO to Collect PHI

a. *Public Health Act* (PHA) – Establishes the authority and duties of the CHPO. It provides the legal basis for public health surveillance and mandatory reporting of notifiable diseases and conditions.

- Section 35(1)(b) permits the CPHO to collect PHI without consent if the CPHO determines, on reasonable grounds, that it is required for:
  - public health surveillance,
  - development of public health programs,
  - health promotion, or
  - administration/enforcement of the Act.
- Section 35(2) limits the CPHO to collecting only the amount and type of information **necessary** for the stated purpose.
- Section 35(3) allows the CPHO to collect the information from any reliable source.

Important Limitation:

- Section 35 does not compel disclosure — it permits the CPHO to collect, but it does not obligate custodians to provide the data unless the condition is listed as notifiable under PHA regulations.

Section 38 – Disclosure Across Jurisdictions

- The CPHO may disclose PHI to public health officials in other jurisdictions (e.g., Public Health Agency of Canada) if there is a formal agreement, which exists in this case for chronic disease reporting.

a. *Health Information Act* (HIA) – Establishes a legal framework for the collection, use, disclosure and protection of personal health information in the Northwest Territories.

Section 43 – Disclosure Between custodians

- Allows health information custodians to disclose PHI to another custodian (DHSS or its Deputy Minister) for purposes such as public health surveillance under:
  - Section 35 of the HIA (e.g., quality improvement, health system management), or
  - Section 37 (permitted uses by a public body)
- This disclosure must align with the purpose for which the PHI was collected or be consistent with that purpose.

2. Disclosure of PHI for Chronic Disease Surveillance

Although the HIA does not currently define public health surveillance as an authorized disclosure or use, the CPHO can lawfully receive PHI about chronic diseases from the NTHSSA under the following conditions:

- The CPHO has reasonable grounds that the information is required for public health surveillance, per section 35(1)(b) of the PHA.
- The health information custodian of the Electronic Medical Record (EMR) must agree to the disclosure of PHI for this purpose.
- The request should comply with the HIA, specifically section 43, which allows a health information custodian to disclose PHI to another custodian (like the DHSS) for uses authorized under sections 35 or 37, including public health surveillance.

3. Comparative Jurisdictional Review

Alberta- *Health Information Act* (HIA)

Alberta's HIA explicitly defines "public health surveillance" and clearly authorizes custodians to disclose PHI to public health authorities without consent.

British Columbia – *Personal Health Information Access and Protection of Privacy Act* (E-Health Act)

Under BC's *Public Health Act* and associated regulations, PHI may be disclosed for public health monitoring and surveillance. *The E-Health Act* also authorizes collection and use of PHI to manage chronic disease at a population level and supports centralized health data systems for population health analytics.

Ontario- *Personal Health Information Protection Act* (PHIPA)

Ontario's *PHIPA and Health Protection and Promotion Act* work together to define and authorize disclosure of PHI for public health surveillance, including chronic disease registries.

4. Recommendations and Legislative Options

- Policy Development: Develop a public health surveillance policy to formalize processes for chronic disease data collection and ensure compliance with the "minimum necessary" principle under both Acts.
- Public Transparency: Communicate with the public regarding how and why chronic disease data is used, especially when collected without consent, to maintain public trust.
- Interdepartmental Agreements: Ensure data-sharing agreements or memorandums of understanding (MOUs) between HSSAs and the DHSS are in place and up to date.
- Amend HIA to explicitly define public health surveillance as authorized use and disclosure of PHI.

CONCLUSION

The current legal framework allows for the disclosure of PHI to the CPHO under section 35 of the PHA for public health surveillance of chronic diseases without individual consent, provided:

- There are reasonable grounds for the collection,
- The amount of data is limited to what is necessary, and
- The custodian agrees to provide the information.

However, the lack of a statutory definition of public health surveillance in HIA may contribute to uncertainty about the scope of such disclosures. Consideration could be given to amending the legislation to include an express definition of public health surveillance in future amendments to enhance clarity.

2.5. ACCESS TO AND CORRECTION OF PERSONAL HEALTH INFORMATION

The HIA defines access and collection requests of personal health information (PHI) as:

“access request” means a request under subsection 96(1) by an individual for access to a record contain personal health about him or her

“correction request” mean a request under subsection 119(1) by an individual for correction of a record containing personal health information about him or her

“applicant” means an individual who makes an access request or a correction request”

A record is defined as:

“A record of information in any form that is made and stored in any manner, such as a written record, electronic record, handwritten or electronic note, audio visual recording, drawing, book, prescription, patient chart, photograph or x-ray or their diagnostic image”

Access to PHI is outlined in sections 94-109 of HIA:

Under HIA, individuals have the right to access their PHI in the custody of a health information custodian. This includes information that is documented in:

- Hard copy
- Electronic copy, or
- Any other media format, including audio records text, digital photography, and
- Any other new or emerging technologies that may be used to store personal health information.

The individual's substitute decision maker also has a right to access the information.

Individuals may request physical copies of their health information, whether paper or electronic, or to examine their record.

There is nothing in HIA that prevents a health information custodian from disclosing PHI with a formal request or a request made verbally.

The HIA sets out the timelines for processing a request for access or requesting a review from the Information and Privacy Commissioner, and associated fees.

Exceptions to Disclosure are outlined in sections 110-118 of HIA:

HIA gives clients the right to access their personal health information. However, certain circumstances are set out when the health information custodian either:

- Must not give access (mandatory exceptions), or
- May not give access (discretionary exceptions).

Mandatory exceptions include:

- Disclosure would reveal PHI about another individual
- Quality Assurance activities
- Disclosure prohibited by the HIA

Discretionary exceptions include:

- disclosure is determined to be harmful to individual or public safety
- information was provided in confidence, and disclosure could lead to the identification of a person who provided the information with the expectation of confidentiality
- information is subject to any kind of privilege of law
- disclosure could prejudice a law enforcement matter
- disclosure would reveal a confidence of the Executive Council or the Financial Management Board
- disclosure could reveal advice, proposals, recommendations, analysis of policy options developed by officials for the Executive Council

Correction of PHI is outlined in sections 119-128 of HIA:

Individuals have the right to request that the information in their health records be corrected if they think it has an error or omission. Health information custodians have a duty to assist the applicant in an open, accurate and complete manner and do so without delay.

A health information custodian cannot charge fees for correction requests.

A custodian who receives a correction request must:

- decide to make the correction or refuse the correction.
- must make a reasonable effort to give the corrected information to anyone it shared the original record within the past year unless deemed unnecessary
- inform any person or organization it shared the records within the past year, that a correction request was received.
- make the correction right away after the decision to grant the correction is made.
- attach a statement of disagreement to their medical record if the custodian refuses the correction.

The HIA sets out the timelines for processing correction requests and requesting a review from the Information and Privacy Commissioner.

FEEDBACK GATHERED

No feedback was received.

DISCUSSION & FINDINGS

The summary of relevant sections from HIA (2.5 Access/Correction of PHI) are here to support stakeholder feedback presented in next section (2.6 Information and Privacy Commissioner) and considered for the HSS.

CONCLUSION

Not applicable.

2.6. INFORMATION AND PRIVACY COMMISSIONER

The powers and responsibilities of the NWT Information and Privacy Commissioner (IPC) are listed in HIA. In conducting a review, the IPC has powers, privileges and responsibilities. The IPC is independent from government and has the power to review the conduct of health information custodians and has recommendation-making powers under HIA.

2.6.1. FEEDBACK GATHERED

Feedback was received from the IPC about eight (8) areas to consider for improvements.

The IPC brought forward the following feedback specific to time extensions:

1. Extend time for custodian response to IPC's recommendation from 30 days to 90 days.
2. Extend time to comply with a decision from 45 days to 90 days.
3. HIA to define "days" to "business days".

According to the IPC feedback these provisions are difficult to implement with existing resources:

4. Reporting privacy breaches to the IPC
5. Section 153- Powers of IPC
6. Section 158 – Requirement to comply with decision

The IPC identified the following provisions are unclear:

7. Section 134 – Request for review
8. Section 89(2) and Section175 – Privacy impact assessment

1. Extend time for custodian response to IPC's recommendation from 30 days to 90 days.

The HIA states that an applicant who makes an access request can request a review by the IPC under Section 141(1) and the IPC will then provide a copy of the review and recommendations under Section 156(1) to the custodian. On receipt of the review the custodian has 30 days to:

a. *(Make a decision whether or not to follow the recommendations of the IPC or some of the recommendations;*
b. *Give note of the decision made under paragraph (a) to the IPC, the individual who requested the review and the Minister; and*
c. *Give notice to the individual who requested the review of the right to appeal referred to in subsection 160(1), if the custodian decides not to follow some of or all of the recommendations of the IPC.*

Feeback received from the IPC for s.156 was that 30 days was insufficient time for the custodian to be able to make considered decisions. The IPC's feedback recommends extending custodian's deadline for a response to 90 days.

2. Extend time to comply with a decision from 45 days to 90 days.

Under s.158 of the HIA, a Custodian has 45 days to comply with a decision made to follow a recommendation made by the IPC in a review report given under subsection 156(1) to the IPC.

Feeback received from the IPC for s.158 was that 45 days was insufficient time for the custodian to comply and implement accepted IPC's recommendations. The IPC's feedback recommends extending custodian's deadline to 90 days.

3. HIA to define 'days' to 'business days'.

HIA does not define the term "days" and currently operates under a timeline that does not differentiate between weekends, statutory holidays or mandatory leave. This can cause a strain in responding to HIA requests, or recommendations depending on when they are received.

The IPC has recommended updating HIA with the inclusion of the definition of days to "business days" to align with the Access to Information and Protection of Privacy Act (ATIPP):

"business day" means any day except:

a. *a Saturday,*
b. *a Sunday,*
c. *a holiday, or*
d. *any day between December 19 and January 5 on which the majority of persons employed in the Office of the Information and Privacy Commissioner are on mandatory leave;*

CONCLUSION

These IPC recommendations to change the timelines are being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.

4. Reporting privacy breaches to the IPC (Harms Test)

DISCUSSION & FINDINGS

IPC feedback reads:

> *"There is no threshold for reporting privacy breaches based on the assessed risk of harm. Every unauthorized collection, use, disclosure, or disposal of personal health information, regardless of the level of risk, must be investigated and reported. Health information custodians are not well resourced to conduct all such investigations on a timely basis and this can have negative consequences: witnesses' memories can fade, information not collected at the time of the breach can be lost, and mitigative measures can be less effective as time passes. At some future date, it may make sense to adopt a risk-based threshold similar to the one in the Access to Information and Protection of Privacy Act."*

- HIA and Regulations governing privacy breach notification

Section 87 of the HIA requires custodians to give notice when an individual's PHI is used or disclosed in an unauthorized manner:

87. Subject to any prescribed exceptions, a health information custodian shall give notice to an individual and, if applicable, to a prescribed person or organization, as soon as reasonably possible if personal health information about the individual is

(a) used or disclosed other than as permitted by this Act;

(b) lost or stolen; or

(c) altered, destroyed or otherwise disposed of without authorization.

Section15 of the HIA Regulations:

15. (1) For the purposes of section 87 of the Act and subject to subsection (2), a health information custodian shall give notice to

(a) the Information and Privacy Commissioner;…

(2) A health information custodian is not required to give notice to the Information and Privacy Commissioner of an incident involving the loss or unauthorised use, destruction or alteration of personal health information if the loss, use, destruction or alteration does not present a reasonable risk of harm to the affected individual.

Subsection 15(2) does provide for instances when notification and reporting is not required to the IPC, however it is limited to PHI loss, unauthorized use, destruction or alteration that does not carry a reasonable risk of harm, and it does not cover PHI collection or disclosure activities. The HIA currently lacks any mechanism to assess level of harm.

This mandatory reporting regime can create regulatory overload and delay meaningful investigations and guidance. It can also create privacy breach reporting fatigue for custodians who may be understaffed and do not have time to conduct substantive inquiries.

- What is a Harms test?

A harms test is an assessment of the materiality of a privacy breach based on the sensitivity of the information. NWT's ATIPPA has recently been amended to include mandatory reporting (s.49.9) of material privacy breaches to the IPC and has included a harms test in legislation to guide the public body in making its determination:

(2) The factors that are relevant in determining whether a breach of privacy with respect to personal information under the control of a public body is material include

a. *the sensitivity of the personal information;*
b. *the number of individuals whose personal information is involved;*
c. *the likelihood of harm to the individuals whose personal information is involved; and*
d. *an assessment by the public body whether the cause of the breach is a systemic problem.*

- Risks of a Harms Test for PHI

PHI has been recognized in Canada as being the most sensitive type of personal information about an individual and can create serious risk if breached, including financial harm, discrimination, mental and emotional distress, and loss of trust in health care systems. Although a harms test may reduce regulatory oversight volume and fatigue, it can carry privacy and governance downsides vs. a mandatory reporting model such as:

a. Subjective decision-making by custodians leading to under-reporting and violation of the law
b. Failure to capture non-tangible or delayed harms
c. Reduced accountability and legal risk management
d. Undermining of patient trust with inconsistencies in interpretation of harm
e. Eroded regulatory oversight for identifying systemic risks and security gaps

- Approach in other jurisdictions – Ontario and Alberta

Ontario

Ontario's PHIPA custodians must report privacy breach to the IPC in seven categories described in the regulations:

- Use or disclosure without authority
- Stolen information
- Further use or disclosure without authority after a breach
- Pattern of similar breaches
- Disciplinary action against a college member
- Disciplinary action against a non-college member
- Significant breach
  - Information is sensitive
  - Breach involves a large volume of information
  - Breach involves many individuals' information
  - More than one custodian or agent was responsible for the breach

Alberta

In 2018, Alberta modified their HIA to require custodians to give notice to the IPC of *any health* information breach that presents a "risk of harm to an individual as a result of the loss or unauthorized access or disclosure". The HIA regulations (s.8.1) outlines factors for custodians to assess risk of harm, including:

- Was the information accessed or viewed by someone?
- Is the information sensitive enough to embarrass someone, hurt them physically, mentally, financially or damage their reputation?
- Could is be used for identity theft or fraud?
- Could the breach interfere with a person's medical care?
- Was the information encrypted?

Importantly, custodians in Alberta do not have to report breaches to the IPC if they can prove:

- The information was accessed or disclosed to another custodian or affiliate;
- They are subject to confidentiality polices that meet the requirements of the legislation;
- Information was not accessed or disclosed for an improper purpose, and;
- Immediate steps were taken to fix the error, and it wasn't further shared.

CONCLUSION

The introduction of a harms test for breach notification has precedence in other Canadian jurisdictions. However, any proposed changes to the legislation introduces legal, ethical, and practical risks, when compared to the current mandatory reporting model, and should be carefully considered to ensure accountability by custodians and maintaining public confidence.

5. Section 153 of HIA - Powers of IPC

IPC feedback received states:

> "When the Commissioner is conducting a review, section 153 requires health information custodians to produce records within 14 days, with no flexibility to extend the time. Practically, this is rarely possible. Often, such prompt response is not strictly necessary. My office typically requests records be produced in one month and frequently receives requests to extend this period. It may make sense to empower the Commissioner with the discretion to extend the time for a custodian to produce records."

6. Section 158 of the HIA - Requirement to comply with decision

IPC feedback received states:

> "When a health information custodian accepts a recommendation in a privacy breach review report, section 158 requires compliance within 45 days of receipt of the decision. However, there is no requirement to report on compliance or steps taken toward compliance. Recommendations are designed to mitigate harm or prevent future privacy breaches. Recommendations generally require action, and some recommendations cannot reasonably be completed in 45 days. It may make sense to require a report on the status of implementation, similar to the provisions in section 49.4 of ATIPP. A longer implementation period with a reporting requirement could help a custodian to develop a realistic workplan and ensure continued focus on achieving compliance."

7. Section 134 – Request for review

IPC feedback received states:

> "When a health information custodian decides not to follow a recommendation in a privacy breach review report, the Act does not require the custodian to give reasons. This creates a challenge if the review was requested by an individual under section 134(1): that individual would have appeal rights, but without reasons it would be difficult for an individual to determine why the decision was made. As a practical matter, health information custodians typically do provide reasons for their decisions, but this should not be discretionary. The health information custodian should be required to provide reasons that explain why it came to its decision."

CONCLUSION

These IPC recommendations regarding processes are being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.

8. Section 89(2) and Section175 – Privacy impact assessment

IPC feedback received states:

> "Privacy impact assessments are required under section 89(2) but the Act provides little guidance: there is no definition, no statement of purpose, nor any directions on when a PIA should be completed, when it should be submitted to the Information and Privacy Commissioner for comment, or what to do with any such comments. At times, my office has received copies of PIAs at or just before implementation of an initiative. An assessment can be a useful planning tool when developed early in the process; when completed at the time of implementation it is little more than a make-work project. Section 175 sets out the Commissioner's ability to provide comments on a privacy impact assessment, but more specific description and direction in the Act would likely improve the value of the PIA as a privacy protection measure."

DISCUSSION & FINDINGS

Section 175 of HIA states:

> *175. The Information and Privacy Commissioner may provide comments to a health information custodian respecting a privacy impact assessment given to the IPC by a custodian under subsection 89(3) or under the regulations."*

PIAs addressing any new information system or communication technology should be completed and submitted early so that there is a reasonable period for review by the IPC and for any comment to be considered by the health information custodian in the planning stages. This period also should have some limits to ensure that the process for commenting do not unreasonably delay projects.

NWT's ATIPPA legislation (s.42.1) may provide a precedence on how to address the timeline of PIA submissions to the IPC, and for custodians to receive review and comments:

> *(2) Subject to subsection (3), a public body shall, during the development of a proposed enactment, system, project, program or service that involves the collection, use or disclosure of personal information, prepare and submit a privacy impact assessment to the head of the public body for review and comment.*
>
> *(3) The head of a public body, with respect to a common or integrated program or service, shall, during the development of the proposed program or service, prepare and submit a privacy impact assessment to the Information and Privacy Commissioner for review and comment.*

CONCLUSION

Tools to provide more clarity for PIA stages are being considered, such as policy amendment or a procedure. Relevant invested organizations, including Office of the IPC, DHSS and HSSAs would be valuable resources to inform these tools.

2.7. OFFENCES AND STATUTE OF LIMITATIONS

Offences and punishment are outlined in sections 185-194 of HIA, which addresses illegal actions related to PHI and penalties for those actions:

- Unauthorized Use of PHI (Section 185)

Prohibits anyone from knowingly collecting, using, or sharing someone's PHI in violation of the Act or regulations.

- Obstruction of the IPC (Section 186)

Prohibits willful obstruction, non-compliance, or making false or misleading representations to the IPC or others in the performance of their duties.

- Record tampering (Section 187)

Prohibits tampering a record by changing, destroying, hiding or falsifying records, or telling someone else to do it, to avoid giving someone access to their health information.

- Misrepresentation (Section 188)

Prohibits obtaining access to or requesting a change to someone's health information by false representation.

- Commercial use (section 189)

Prohibits using PHI for marketing, solicitation or profit without express consent.

- General contravention (section 190)

Prohibits anyone from knowingly breaching any provisions in the Act or regulations.

- Protection from prosecution (section 191)

A person can't be prosecuted if they are following a requirement or recommendation from the IPC.

- Penalties (section 192)

Any person found guilty of contravening of failing to comply with the Act or regulations may be liable and punished as follows:

- A corporation can be fined up to $500,000;
- An individual can be fined up to $50,000.

- Corporate Officers may be responsible (section 193)

If a corporation breaks the law, then anyone in the company who helped make it happen can also be personally charged and fined, even if the corporation itself isn't prosecuted.

- Time Limit (section 194)

Charges under this Act must be laid within three years from the date the offence occurred. After that, you can't be prosecuted.

2.7.1. ADDITION OF A "SNOOPING" OFFENCE

In the context of healthcare, "snooping" refers to intentional unauthorized access to PHI by a person who has no legitimate need to know that information as part of their job or duties. It is often done out of curiosity, personal interest, or malice—and not for the care or treatment of the patient. Snooping erodes trust and confidence in healthcare providers and systems, can expose sensitive personal information leading to embarrassment, discrimination or harm, and potentially, be used for identity theft or fraudulent activities.

DISCUSSION & FINDINGS

1. Current wording of Section 192

The HIA imposes a general clause to address offences and punishment of contraventions of legislation:

> *192. Every person who contravenes or fails to comply with the Act or regulations is guilty of an offence punishable on summary conviction, and except as provided is liable*
> *(a) in the case of a corporation, to a fine not exceeding $500,000; or*
> *(b) in the case of any other person, to a fine not exceeding $50,000.*

The broad scope of this section covers both intentional and unintentional noncompliance but does not distinguish snooping as a separate offence.

2. Legal rationale for separate snooping clause

a. Clarity in statutory interpretation

The addition of a separate clause defining snooping provides a more precise legal definition of the offense for the purposes of prosecution of offences and statutory limitations.

b. Recognition of unique harm

An explicit offence for snooping recognizes snooping as a serious wrongdoing with significant consequences which may further deter employees from accessing PHI without authorization.

c. Proportional and tailored penalties

Snooping violations can be addressed with separate and appropriate penalties to address the severity of the activity.

3. Comparative Jurisdictional Review

Several jurisdictions in Canada have incorporated snooping as a separate offence when revising health privacy legislation.

Jurisdiction	Legislation	Explicit offence	Penalty
Alberta	*Health Information Act*	**Yes – s.107(2)(b)**	Up to $200,000 (individual) / $1,000,000 (corp)
Ontario	*Personal Health Information Protection Act (PHIPA)*	**Yes – s.72(1)(a)**	Up to $200,000 (individual) / $1,000,000 (corp); Jail possible

Manitoba	*Personal Health Information Act*	**Yes – s.63(1)(a)**	Up to $50,000 (individual) / $500,000 (corp)
Saskatchewan	*Health Information Protection Act (HIPA)*	**Yes – s.64(3.1),(3.2)**	Up to $50,000 (individual) / $500,000 (corp); Possible 1 year imprisonment

4. Deeper Dive – Ontario and Saskatchewan Health Legislation

a. *Health Information Protection Act* (HIPA)

Saskatchewan's HIPA legislation explicitly criminalizes employees who wilfully access, use, or direct another person to access or use, PHI not reasonably required to carry out an authorized purpose. If found guilty of an offence and liable on summary conviction, employees are subject to a fine up to $50,000 and/or imprisonment of up to one year. The statute of limitation is 2 years from date of discovery of the offence.

Benefits of specific offence:

- Explicit targeting of curiosity-based, malicious, or intentional access prevents ambiguity and signals seriousness. Employees may mistakenly believe that only accessing but not disclosing client records is not illegal.
- Broad coverage of employees, service providers and directors improve accountability across the health system. Addresses directing others to commit offences.
- Robust penalties, including imprisonment, reinforces deterrence and addresses the seriousness of the activity.

a. *Personal Health Information Protection Act* (PHIPA)

Ontario's PHIPA legislation makes it an offence to willfully collect, use, or disclose PHI in contravention of the legislation or regulations. Penalties are up to a maximum of $50,000 for individuals and/or imprisonment of up to 10 years. There is no statute of limitation for prosecution of offences.

Recent PHIPA reforms in 2020 and 2024 have focused on enhancing enforcement tools by increasing fines, introducing jail time if convicted, and mandating audit logs specifically to deter snooping activities. Additionally, the IPC has been granted the discretion to issue administrative monetary penalties (AMPs) directly as part of their enforcement powers for violations of the Act. AMPs, up to a maximum of $50,000 for individuals and $500,000 for organizations, may be issued for severe violations to encourage compliance or prevent a person from deriving, directly or indirectly, any economic benefit from contravening the law.

Benefits of this approach:

- Supports transparency and trust in health care systems by underscoring accessing PHI without authorization is a serious violation.
- Effectively covers snooping under "wilful collection" and enabling prosecution for unauthorized access even if no disclosure occurred.
- Gives discretion to the IPC to sanction individuals for serious violations directly.

CONCLUSION

The act of snooping in sensitive PHI by employees in a position of trust is an abuse of power and can significantly erode trust in the health care system.

To align with other jurisdictions in Canada, and to recognize the seriousness of snooping activity, consideration should be given to introducing a separate clause in the HIA to criminalize intentional unauthorized access to health records with proportionate penalties. Additional consideration of administrative monetary penalties as a potential enforcement mechanism should be reviewed.

Part 3 – Emerging Themes

Several issues have emerged during this review period.

3.1. INDIGENOUS DATA SOVEREIGNTY

Indigenous Data sovereignty, as understood at the time of writing this report, is generally that Indigenous people individually and collectively as Indigenous groups have the right to control their own data about themselves and their way of life and knowledge. They have the right to access information about them regardless of where it is housed. Understanding of this term and approaches to it in NWT and elsewhere is evolving.

FEEDBACK GATHERED

Feedback[8] suggested that the HIA review should include Indigenous data sovereignty and OCAP® principles as a critical lens. Another suggestion received is that existing health privacy legislation is often a barrier to communication between different parties that have legitimate roles in supporting a client (e.g. service providers within Indigenous governments).

DISCUSSION & FINDINGS

There is great interest by Indigenous governments and organizations to have access to information of their members. The HIA only currently applies to an individual's access to their own health information. Collective information that is de-identified can currently be disclosed, if that information will not re-identify any individual.

More work needs to be done to consider how to incorporate Indigenous data sovereignty directly into the HIA. It is noted that other health information legislation in Canada has yet to directly address Indigenous data sovereignty. HSS may want to consider NWT interpretations, while also considering aligning with approaches from other jurisdictions.

In the meantime, section 60 allows DHSS to share health information with Indigenous governments for health services, on a government-to-government basis. Section 60 of HIA states:

[8] OCAP is a registered trademark of the First Nations Information Governance Centre, online at <https://fnigc.ca/>. The principles refer to the concepts of ownership, control, access and possession of First Nations' data and information.

> "Subject to the regulations, the Department may disclose personal health information about an individual for the purpose of the development of health programs or services, or for the management, monitoring or evaluation of the health system or health programs or services, to
>
> *(a) the Government of Canada, a government of a province or territory, or an Aboriginal government; or*
> *(b) a department or other organization of a government referred to in paragraph (a)."*

This section could be used to start sharing health information more directly, if it has not already. This may not address sharing directly to the service providers of the Indigenous governments.

The next time the HIA is amended, the terminology of Aboriginal government may be updated to reflect current terms (e.g. Indigenous). In future, consideration should be given to whether "Indigenous organization" should be included as entities on behalf of Indigenous people that should be permitted to receive PHI.

3.2. ACCESS TO PERSONAL HEALTH INFORMATION VIA "PATIENT PORTALS"

Under HIA, individuals have the right to access their PHI. Currently in NWT, upon request, individuals are provided with a copy of their records, or they can view their records at a health facility. Copies of health records are provided on paper printouts, electronic copies in PDF, CD or USB stick, in accordance with the Regulations. Requests for records can be made at any health center or hospital where they receive(d) care.

FEEDBACK GATHERED

Feedback was received from clients, as well as media reports, indicating that NWT residents want access to their health information online through a patient portal or other electronic means.

DISCUSSION & FINDINGS

Patient portals are secure online platforms that provide patients with access to their PHI, such as immunization records, lab results, medication lists, etc. Some portals include appointment booking options, or prescription refill request functionality.

The benefit of this approach is patients can access their information without attending a health centre to make a request, they can see all their cumulative results, and they can access the portal from anywhere there is the Internet, including when out of the NWT. There is some evidence that patients have better experience when they are able to be more involved in their care with access to their own information.

Currently in Canada, patient portals are available in 6 provinces (Alberta, British Columbia, Saskatchewan, Ontario, Prince Edward Island and Quebec) and there has been growing expectations in the NWT that individuals will one day be able to access their information in this manner.

CONCLUSION

The NWT's existing eHealth systems are currently unable to provide access via patient portals, but it is the intent that as systems are updated or replaced, these new applications will have the technological ability to support the creation of a patient portal.

3.3. FEDERAL GOVERNMENT INITIATIVES

FEEDBACK GATHERED

Several initiatives will impact health information legislation:

- Substantial Similarity Status with *Personal Information Protection and Electronic Documents Act* (PIPEDA)
- *Canadian Health Data Charter* and data stewardship
- National focus on sharing between continuing care providers

DISCUSSION & FINDINGS

1. Substantially similar status

Between 2022- 2024, amendments were introduced by the Federal government to PIPEDA. These amendments, if passed into law, would have meant changes to the HIA in order to obtain substantial similarity status with the revised PIPEDA. These amendments to PIPEDA died on the order paper when Parliament dissolved on January 6, 2025.

DHSS has been working at various times toward obtaining substantial similarity status from the Federal Government. Applying for and obtaining this status would permit pharmacists and physicians with their own businesses outside of the government health system to follow the NWT HIA requirements and not PIPEDA as well.

DHSS may want to consider if substantial similarity status is something that should still be applied for.

2. Data stewardship

The *Pan-Canadian Health Data Charter* was published by the federal government in October 2023. This charter is agreed to by all federal, provincial and territorial governments, except Quebec. As part of the Data Charter, there is a move towards health data stewardship, and away from custodianship. DHSS has been participating in ongoing work to set a Pan-Canadian Health Data Stewardship Framework. In future when this work is finalized, changes to the HIA will need to be considered.

3. National focus on Continuing Care Services

Since the Covid-19 pandemic began in 2020, the federal government has been investing in and working towards a *Safe Long Term Care Act.* This has put a more national focus on the continuing care spectrum (from home care to supported living, to long term care), when most continuing care services are funded by the provinces and territories, with some funds from the federal government through health transfer. Feedback was received that more consideration in HIA is needed of the ability to share information in the continuing care sector with other health or social services providers across the care settings to be able to address complex needs among older adults.

In the NWT, with the exception of AVENS, all of the long-term care facilities are run by the HSSAs.

3.4. GNWT SERVICE INTEGRATION

In March 2025, the Premier of the NWT raised awareness about GNWT shifting the way it provides services to residents across the NWT through a whole-of-government service integration initiative to improve access to services. Information sharing is critical piece to allow for more person-centered support and care.

DISCUSSION & FINDINGS

Work exploring how service integration can be implemented under the existing HIA framework is underway. DHSS is actively engaged in the service integration initiative recognizing the importance of seamless information sharing within GNWT to improve the experiences of services users in the NWT while remaining compliant with current privacy legislation. It is noted that a future amendment of HIA directly supporting service integration between GNWT departments and agencies may be beneficial.

3.5. DATA OWNERSHIP AND ARTIFICIAL INTELLIGENCE

The advancement of artificial intelligence is rapidly reshaping healthcare by automating complex tasks, augmenting clinical decision-making, and enabling personalized treatment. AI has the potential to improve health outcomes and system efficiencies. However, these advancements rely heavily on access to large volumes of PHI like patient medical history, test results, imaging and genetic data, which is legally protected through HIA. The data-driven nature of AI raises concerns around health privacy, data security, regulatory compliance, and possible re-identification of de-identified data.

DISCUSSION & FINDINGS

1. Legislative landscape

Canada's proposed *Artificial Intelligence and Data Act* was expected to provide a regulatory framework as part of Bill C-27 but failed to pass in 2025. In the interim, the federal government has

issued a Voluntary Code of Conduct for advanced generative AI, which offers guidance but creates no legal obligations. This gap in industry regulation creates a risk for inherently sensitive PHI. The introduction of AI systems using health data beyond the original purpose of collection, or without patient's being fully informed, could potentially contravene the HIA and undermine the patient's legal control over their information.

2. Re-identification risks

Re-identification of data is also a significant concern. Health information may be de-identified for research or reporting purposes, but this is not the same as anonymization when AI is working with:

- Datasets containing unique or rare combinations
- Systems with access to external datasets that could be used for cross-referencing or data-matching
- Populations that are small or geographically concentrated like the NWT
- Predictive models that deduce sensitive traits by attribute referencing

3. Secondary use creep

Additional risks of AI are secondary use creep. Currently, custodians may use PHI from an individual without consent for internal management purposes and health system management (s.35 and s.37). However, if the PHI is collected for one purpose like patient care and then used later to train AI algorithms or shared with third parties for research, the boundaries of lawful use begin to blur and may lead to unauthorized secondary use.

4. Security risks

AI tools rely on cloud computing platforms for data processing and storage which creates external vulnerabilities if the vendor has insufficient security, or stores data in foreign jurisdictions. Section 85 of the HIA requires custodians to maintain reasonable administrative, technical, and physical safeguards for the protection of PHI which means they are accountable if the information is breached.

5. Auditing

Many AI systems operate as "black boxes". Deep learning models use layers of interconnected nodes to transform input data into outputs making it difficult to determine:

- What data the model accessed,
- How it makes decisions,
- If it retains or misuses data

This limits the ability to audit AI systems for privacy violations or provide a mandatory record of activity which custodians are currently obligated to do when it comes to PHI.

CONCLUSION

The integration of AI into healthcare offers the potential for advancement in care and patient outcomes, but it also presents significant privacy challenges in the context of the NWT, where small populations and geographic isolation increase the risk of re-identification from de-identified data.

The HIA gives individuals the right to control their PHI and any use of that information by AI systems must be compliant with legislation.

Part 4 – List of Conclusions

This part of the Report summarizes the conclusions made throughout the document. The conclusions are listed in alignment with the HIA order of parts and sections.

Topics for Consideration	Conclusions / Considerations	Recommendations
HIA PART 1 – INTERPRETATION AND APPLICATION		
Adding new terms into definitions	Each submission from the invested organizations on proposed changes to existing definitions or introducing new terms would benefit from completing an assessment from the 'value added' perspective and its substantiation when measuring beneficial impact on ongoing improvements of the HIA and its interpretation.	More work and engagement for appropriate legislative amendment.
HIA PART 2 – ROLES AND RESPONSIBILITIES		
Adding other health care professionals as health information custodians	Additional health information custodians can be added as needed to the Regulations. Policy work is needed to determine which additional custodians should be added.	More work and engagement for appropriate legislative amendment.
Custodians that are not employed by the GNWT are not aware they are custodians and subject to the HIA	The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution. Additional private health information custodians can be added as needed to the Regulations. More policy work is needed to determine if an exhaustive list of custodians is desired, and which private custodians should be added.	A policy tool should be developed.

Public Guardian to be considered as a custodian	The issue lies not with the legislative framework of the HIA but with the position of the Public Guardian within the DHSS. Policy work is needed to determine whether amendments to the HIA or the *Guardianship and Trusteeship Act* would be most appropriate.	More work and engagement for appropriate legislative amendment.
HIA PART 3 – CONSENT AND SUBSTITUTE DECISION MAKERS		
Mature minor consent when addressing complex issues (age indication for mature minor)	The HIA is aligned with common law in other jurisdictions in Canada, however other resources and training should be considered to assist custodians to guide assessment of minors' maturity.	A policy tool should be developed.
The consent section is long and complex	The length of the consent part is in line with other Canadian jurisdictions. Policy work should be done to see if these sections of the HIA can meaningfully be simplified.	A policy tool should be developed.
Some HIA provisions cannot be implemented with existing resources (consent conditions)	Amending the HIA will not solve the use of consent conditions in a particular eHealth system. Funding by the GNWT for system enhancement is outside of the scope of legislation.	N/A
HIA PART 4 – COLLECTION, USE, DISCLOSURE AND PROTECTION OF PHI		
Use of mobile devices to disclose images for consultation	The current HIA adequately addresses the use and disclosure of patient photographs for consultation purposes. The issue lies not with the legislative framework but with implementation and compliance. Strengthening training, policy and procedure enforcement is the most effective and proportionate solution.	A policy tool should be developed.

Collection/Use/Disclosure of PHI for Cancer Surveillance Program	While the intent of the Territorial Cancer Surveillance program is aligned with preventative health objectives, the current provisions of the HIA and Regulations do not clearly permit the collection, use and disclosure of PHI for the purpose of directly contacting average-risk individuals for cancer screening. Consideration could be given to amend the HIA Regulations to include a specific provision authorizing the disclosure of PHI for the purposes of organized population-based screening programs.	More work and engagement for appropriate legislative amendment.
Disclosure of PHI for joint Guardianship and Trusteeship applications	The current legislative framework creates practical and legal challenges in preparing joint guardianship and trusteeship applications due to limits on the disclosure of personal health information. Amending the *Guardianship and Trusteeship Act* would more directly and effectively address the issue of PHI disclosure in this context, ensuring timely and lawful access to necessary information. However, consideration could also be given to amending the HIA to permit limited, purpose-specific disclosure where doing so would benefit the client.	More work and engagement for appropriate legislative amendment.
Disclosure of PHI to the NWT Leadership Council	Under HIA, there is no authority for health information custodians to disclose identifiable PHI to the NWT Health and Social Services Leadership Council without consent. However, the Council's oversight and advisory role can be fully supported using de-identified information.	No further work is needed.

Disclosure of PHI to other government bodies	Under the current HIA, health information custodians are not authorized to disclose identifiable PHI to ECE or EIA for schools, income support, or integrated service delivery purposes without the individual's consent. More policy work is needed to identify the scope of policy or legislative amendments to appropriately target such a disclosure for these purposes. Other Canadian jurisdictions have addressed this issue through targeted amendments and multi-agency frameworks that balance service integration with privacy protections.	More work and engagement for appropriate legislative amendment.
Jurisdictional Clarification of Section 50(b) of HIA	Section 50(b) of the HIA would benefit from a legislative amendment in the future to explicitly state that only subpoenas, warrants, and legal orders enforceable within NWT jurisdiction authorize the disclosure of PHI without consent. This would align the HIA with best practices in jurisdictions like Alberta and provide certainty to custodians. As a secondary option, in the absence of an amendment, custodians should adopt a formal policy or SOP requiring verification of jurisdictional validity before disclosing PHI in response to legal instruments. This would help ensure lawful disclosure, support consistent decision-making, and uphold the privacy principles underlying the HIA.	A policy tool should be developed.

Managing Public Health Outbreaks and Duty of Care	The HIA and *Public Health Act* PHA in the NWT provide a legally sufficient and nationally aligned framework for the disclosure and use of PHI during public health outbreaks such as measles. Disclosure to public health officials is authorized without consent under Section 66 of the HIA, referencing the clear authority granted under the PHA. Furthermore, physicians may access the immunization status of their patients as part of providing care and are ethically obligated, under the duty of care, to use that information to protect patients' health. The existing legislative framework aligns with other Canadian jurisdictions and adequately supports both public health surveillance and clinical responsibilities.	There is no demonstrated requirement to amend the HIA to support these functions. Amendments to PHA would require separate consideration.
Public Health Surveillance	The current legal framework allows for the disclosure of PHI to the Chief Public Health Officer under section 35 of the *Public Health Act* for public health surveillance of chronic diseases without individual consent, provided: • There are reasonable grounds for the collection, • The amount of data is limited to what is necessary, and • The custodian agrees to provide the information. However, the lack of a statutory definition of public health surveillance in HIA may contribute to uncertainty about the scope of such disclosures. Consideration could be given to amending the legislation to include an express definition of public health surveillance in future amendments to enhance clarity.	More work and engagement for appropriate legislative amendment.

HIA PART 5 – ACCESS TO AND CORRECTION OF PERSONAL HEALTH INFORMATION HIA PART 6 – REVIEW AND APPEAL HIA PART 7 – INFORMATION AND PRIVACY COMMISSIONER		
Extend time for health information custodian response to IPC's recommendation from 30 days to 90 days.	These IPC recommendations to change the timelines are being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.	More work and engagement for appropriate legislative amendment.
Extend time to comply with a decision from 45 days to 90 days.		
HIA to define 'days' to 'business days'.		
Reporting privacy breaches to the IPC (harms test)	The introduction of a harms test for breach notification does have precedence in other Canadian jurisdictions. However, any proposed changes to the legislation introduces legal, ethical, and practical risks, when compared to the current mandatory reporting model, and should be carefully considered to ensure accountability by custodians and maintaining public confidence.	
Section 153- Powers of IPC	These IPC recommendations regarding processes are still being evaluated for impact on the rest of the HIA, to be put forward in the legislative process in the future.	
Section 158 – Requirement to comply with decision		
Section 134 – Request for review		
Section 89(2) and Section175 – Privacy impact assessment	Tools such as policy amendment or a procedure able to provide more clarity for PIA stages are being considered. Relevant invested organizations, including Office of the IPC, DHSS and HSSAs would be valuable resources to inform these tools.	A policy tool should be developed.

HIA PART 8 – GENERAL		
Addition of a 'snooping' offence	The act of snooping in sensitive PHI by employees in a position of trust is an abuse of power and can significantly erode trust in the health care system. To align with other jurisdictions in Canada, and to recognize the seriousness of snooping activity, consideration should be given to introducing a separate clause in the HIA to criminalize intentional unauthorized access to health records with proportionate penalties. Additional consideration of administrative monetary penalties as a potential enforcement mechanism should be reviewed.	More work and engagement for appropriate legislative amendment.

For more information, please visit:

www.hss.gov.nt.ca

or email at **hsscommunications@gov.nt.ca**