Yukon Information and Privacy Commissioner

Health Information Privacy and Management Act

2020 Review

Information and Privacy Commissioner's Comments and Recommendations

This page has been intentionally left blank.

Table of Contents

Origins and overview of the Yukon's *Health Information Privacy and Management Act*

Since 2016, Yukoners' personal health information (PHI) has been governed by the *Health Information Privacy and Management Act* (HIPMA). HIPMA was created with the acknowledgement of the special status our PHI holds in comparison to other kinds of personal information (PI). PHI is the most sensitive kind of PI because (in contrast to a credit card number, for example) the information is intrinsically about you and reveals some of your most sensitive characteristics (e.g., medical diagnosis), and cannot be readily changed to avert harm in the case of an unauthorized disclosure. Because of this property, PHI is highly valued, and access is sought by individuals, medical professionals, researchers, corporations, and cybercriminals alike, albeit for different reasons.

The purposes of HIPMA are:

> *(a) to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information;*
>
> *(b) to establish rules for the collection, use and disclosure of, and access to, personal health information that protect its confidentiality, privacy, integrity and security, while facilitating the effective provision of health care;*
>
> *c) subject to the limited and specific exceptions set out in this Act, to provide individuals with a right of access to their personal health information and a right to request the correction or annotation of their personal health information;*
>
> *(d) to improve the quality and accessibility of health care in Yukon by facilitating the management of personal health information and enabling the establishment of an electronic health information network;*
>
> *(e) to provide for an independent source of advice and recommendations in respect of personal health information practices, and for the resolution of complaints in respect of the operation of this Act; and*
>
> *(f) to provide effective remedies for contraventions of this Act.*[1]

HIPMA establishes rules for authorized collection, use and disclosure of PHI and for its protection. It provides individuals with right of access to their records. The Act also aims to improve quality and accessibility of healthcare in recognition that health care in Canada is publicly funded. It also establishes a framework for the development of an electronic health information network. Lastly, it provides for independent oversight by the Yukon's Information and Privacy Commissioner (IPC), to ensure compliance with its provisions and contains measures to address any non-compliance.

[1] Section 1 of HIPMA.

The social and technological context for the provision of healthcare has changed since the inception of HIPMA. The COVID-19 pandemic has given rise to or accelerated developments that impact PHI such as remote healthcare, digital contact tracing and exposure notification, the idea of digital vaccination passports and, coincidentally, accelerated adoption of underlying technologies such as cloud computing, the internet of things (IOT), and artificial intelligence (AI). Developments in genomics[2] are opening up a new frontier for PHI. These challenges and their solutions create new privacy risks. This new landscape requires amendments to HIPMA's provisions to ensure it will continue to achieve its purposes.

Custodians who are bound by the Act have encountered challenges in its implementation. In working with custodians, our office has received feedback and spotted provisions that can be improved to facilitate understanding and compliance.

In terms of oversight, the IPC has encountered issues that need to be addressed through amendment to ensure the IPC can effectively fulfill their mandate.

For all of these reasons, namely socio-technical developments and systemic experience of Yukon entities and the IPC with the Act, review of the Act is both timely and necessary.

Innovations and developments in health care that impact privacy

Although geographically quite isolated, the Yukon's healthcare is connected to and influenced by worldwide developments. In the following paragraphs, the most significant developments are highlighted.

Social and environmental development

COVID-19

A pandemic such as COVID-19 has not been seen in the past hundred years and has created challenges for modern healthcare. There are many tools available that were not around during earlier pandemics or that were not needed during smaller scale epidemics. There has been rapid adoption and deployment of these tools since early 2020 and additional tools are in active development. One of the most striking effects has been the rapid adoption of already available health care supporting solutions that leverage cloud computing technologies, the internet of things (IOT), and artificial intelligence (AI). Examples include remote healthcare solutions, audio and video conferencing with health care providers, and symptom and cure check algorithms. New digital tools developed specifically for the COVID-19 pandemic include contact tracing and exposure notification applications and digital proofs of vaccination. Each of the aforementioned technologies can create challenges for the protection of privacy and access to records. Some of the more generic technologies that have received a boost from the pandemic are discussed in the section of this document on digital transformation. Below I discuss

[2] Medical treatments tailored on the basis of a person's DNA.

some of the technology that was developed specifically in response to the pandemic.

Contact tracing and exposure notification

Although contact tracing applications have not been actively implemented in the Yukon, Yukoners are able to install contact tracing apps on their phones. The Office of the IPC monitored the development of contact tracing and exposure notification applications in 2020. Problems with these apps can include flaws in their design that make them vulnerable to tracking and surveillance beyond the limited use of exposure notification.[3] Also, the creation of fake versions of official apps can lead to the compromise of PI or extortion by ransomware.[4] The official Canadian contact tracing application was reviewed by privacy commissioners in Canada. Privacy best practices were incorporated into its design, such as a limitation of its functions to exposure notification, as opposed to contact tracing, and it does not use GPS to track the individual. While these apps may be useful in larger centres in support of contact tracing by public health officials, the effectiveness of exposure notification applications in rural areas is still up for debate.

Digital proof for travel

With the pandemic in its second year, the pressure mounts on policy makers to open the economy and facilitate travel for that part of the population that has been vaccinated. Vaccine passports, certifications or the like have been identified as a potential solution. Many organizations, including several airlines, the government of Denmark, digital-ID companies, and the World Economic Forum, are already building or acquiring solutions that will require vaccination records and/or test results to issue some sort of proof that will allow individuals to travel.[5] Academics have raised concern regarding the effectiveness, legitimacy, and feasibility of the proposed solutions. Below are some of the concerns raised.

- Vaccination likely does not completely prevent but only reduces the chance of an inoculated person spreading COVID-19.[6] Until more proof of vaccine effectiveness is available and thus a stronger rationale for necessity is provided, it may be hard to establish a legitimate purpose for the collection, use and disclosure of PHI in relation to COVID-19 vaccination passports.
- Access to vaccines may not be equitable across populations, and certain groups may choose not to get vaccinated for religious or other personal reasons. Providing travel benefits to those who are vaccinated creates the risk of stratification between those in the population who have the ability to travel and those who do not, and will require making a distinction between both groups by tracking who has and who has not been vaccinated.
- It will be difficult and time-consuming to develop a system that is able to accurately and reliably validate proof of vaccinations both in Canada and amongst foreign travelers.

---

[3] https://www.darkreading.com/application-security/contact-tracing-apps-still-expose-users-to-security-privacy-issues/d/d-id/1339685.

[4] https://nationalpost.com/news/canada/hackers-target-canadians-with-fake-covid-19-contact-tracing-app-disguised-as-official-government-software.

[5] https://www.washingtonpost.com/lifestyle/travel/yellow-card-vaccine-passport/2020/12/30/746c0558-40b7-11eb-8db8-395dedaaa036_story.html.

[6] https://coronavirus.jhu.edu/vaccines/vaccines-faq.

- Such a system will inadvertently carry privacy risks and create dilemmas regarding the authority to collect and use such information, retention, and who should operate the system.
- Proposed decentralized solutions for vaccination passports, such as the use of blockchain technology, carry additional privacy and accuracy risks.[7]

Aging populations

The World Health Organization asserts in its Global Health and Aging report:[8]

> *The world is on the brink of a demographic milestone. Since the beginning of recorded history, young children have outnumbered their elders. In about five years' time, however, the number of people aged 65 or older will outnumber children under age 5.*[9]
>
> *The number of people aged 65 or older is projected to grow from an estimated 524 million in 2010 to nearly 1.5 billion in 2050, with most of the increase in developing countries.*[10]

The report asserts that these increased numbers of elderly people will both live longer and require more medical attention because they will accumulate more chronic conditions during these years.

For the Yukon, the same trend becomes clear from Statistics Yukon demographic projections,[11] showing a much stronger increase in the 55+ segments over the next 20 years, compared to the other segments.

Consequently, the cost of maintaining a quality healthcare system will increase and put pressure on policymakers to offset some of these costs. A likely candidate for cost savings is the use of all kinds of technology to optimize time spent by healthcare providers (e.g., connected health care solutions including patient monitoring and AI-based diagnosis and treatment recommendations) and to reduce overhead (e.g., health care delivered via video conferencing instead of in-person visits with doctors and online scheduling). Some of these technologies have already been made available to some Yukoners.

Although an aging population does not create new privacy risks in and of itself, like COVID-19, it may tip the momentum in favor of (rapid) adoption of new technologies. Although aimed at reducing costs or optimizing outcomes, care must be taken to ensure these technologies do not infringe on the rights of individuals (including their right to privacy and access to their PHI) or create unmitigated risks to the protection of privacy.

---

[7] Many of these issues are currently being addressed by the World Health Organization. See: https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers.

[8] Global Health and Aging, World Health Organization, National Institute on Aging, National Institutes of Health, U.S. Department of Health and Human Services, October 2011, located at: https://www.who.int/ageing/publications/global_health.pdf#page=7&zoom=auto,-274,748.

[9] *Ibid.,* Overview.

[10] *Ibid.,* Overview.

[11] https://yukon.ca/en/population-projections-2020-2040-sep-2020.

Digital transformation

Many health care solutions rely on new technologies leveraging a combination of IOT, Cloud and AI. Each of these technologies create distinct risks for privacy protection and access; these risks can compound when a combination of technologies is used.

Cloud computing

Use of a cloud for information storage creates risks to accessing information and for privacy protection.

Most cloud service providers are situated in jurisdictions outside Canada. Cloud service providers, particularly those offering public cloud solutions,[12] will generally offer "take it or leave it" contracts which severely limits the ability of custodians to ensure the risks to privacy are properly addressed through contract: control of the PHI; restricting the collection, access, use and disclosure of the PHI by the cloud providers' employees; securing the PHI and what will occur in the event of a breach; retaining the PHI during the contract term; ensuring the integrity and accessibility of the PHI; and the return or secure destruction of the PHI upon termination of the contract. How the laws of the jurisdiction where the data is stored will impact the privacy of the PHI must also be considered.

Access to information stored in the cloud may be impeded if the cloud service is unavailable,[13] the information is lost, or the cloud provider goes out of business.

The internet of things

The number of devices, small and big, with a connection to the internet, has increased drastically over the past four years.[14] This development has been named the rise of the internet of things (IOT). The introduction of anything from smart watches, cars and fridges to intelligent thermostats and lamps will ensure our lives will be more connected than ever in the years to come. IOT devices have also made their way into the healthcare industry. Increasingly, all sorts of connected devices are used in medicine and the treatment or monitoring of patients. In the Yukon, there are already several programs that use some form of remote monitoring of patients. These connected devices have the potential to increase accessibility and quality of care, especially for remote locations.

As with most new technologies, there have been plenty of incidents with IOT devices in a healthcare setting. A survey conducted by Irdeto[15] stresses this fact and shows that in 2019 the healthcare industry

---

[12] Public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Mell, P. and Grance, T., Special Publication 800-145, U.S. Department of Commerce, September 2011, at p. 3.

[13] October 22, 2012, Flipboard, Foursquare, Netflix, Pinterest, and Instagram services were unavailable when the cloud service providers' servers went down. Amazon Cloud Service Goes Down and Takes Popular Sites With It, Perlroth, N., Bits, October 22, 2012, http://bits.blogs.nytimes.com/2012/10/22/amazon-cloud-service-goes-down-and-takes-some-popular-web-sites-with-it/?_r=0.

[14] In 2018 there were 7 billion IoT devices. In 2020, experts estimate the installation of 31 billion IoT devices: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2, at p.2.

[15] Irdeto Global Connected Industries Cybersecurity Survey (2019) Irdeto.

suffered the most cyberattacks against its IOT devices compared to other industries.

Data stored within IOT enabled devices (or the devices themselves) can be stolen. This makes PHI susceptible to cybercriminals who run elaborate campaigns to compromise these IOT devices and the networks on which they operate. The captured PHI has been used to make fraudulent health claims and to create fake (medical) IDs for buying and selling drugs.

In *Sherman Estate v. Donovan*, 2021 SCC 25, the Supreme Court of Canada (SCC) recognized the risks to privacy that arise from the internet. Most solutions used to deliver remote care or to disseminate personal health information to custodians or patients are web-based. In reference to the internet's contribution to increased privacy risks to individuals, the SCC stated, "the growth of the Internet, virtually timeless with pervasive reach, has exacerbated the potential harm that may flow from incursions to a person's privacy interests"[16] adding that "a risk to personal privacy may be tied to a risk of psychological harm".[17]

There are other risks with IOT besides protection of privacy. IOT devices may in some instances receive updates or commands from the provider that alter the type, frequency or purpose of the data collected. IOT devices may locally cache PHI. Aside from the risk of breach, it also poses a challenge for retention requirements as secure and timely destruction of information must be ensured.

Artificial intelligence

Artificial Intelligence (AI) in healthcare takes on different forms. It has beneficial uses in the analysis of compounds for the creation of new medication, as a means to analyze symptoms to create diagnoses and treatment plans and as an integration to work together with IOT devices and cloud connectivity. The latter example is illustrated by smart insulin pumps which are connected to the cloud, where data is analyzed with the help of AI to create a personalized working of the insulin pump optimized to the situation of a specific patient.[18]

With certain AI deployments (e.g., insulin pump), physical harm is a possibility (e.g., wrong diagnosis) and the stakes are higher. As such, there needs to be routine checks and balances to prevent harm.

In a recent report *Getting Ahead of the Curve: Meeting Challenges to Privacy and Fairness Arising from the Use of Artificial Intelligence in the Public Sector*, issued by the Yukon Ombudsman and Information and Privacy Commissioner together with the British Columbia (BC) Ombudsperson and the Information and Privacy Commissioner for BC, the risks and benefits associated with the use of AI are highlighted and recommendations are provided to facilitate responsible use that include legislative reform to privacy laws.

---

[16] *Sherman Estate v. Donovan*, 2021 SCC 25, at para. 51 citing *Douez v. Facebook, Inc.*, 2017 SCC 33, [2017] 1 S.C.R. 751, at para.59.
[17] *Ibid.* at para. 54, citing *Bragg* (para.14; see also J.Rossiter, Law of Publication Bans, Private Hearings and Sealing Orders(loose-leaf), s.2.4.1).
[18] https://www.mddionline.com/digital-health/how-ai-personalizing-insulin-therapy-diabetes-patients and https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

Genomic medicine

Another recent advance in healthcare is the better understanding of the human genome. With the help of AI, vast data repositories of genomic information, and cloud computing processing capabilities, scientists are able to learn much more from a DNA sample than before. DNA samples are already being used to detect or predict diagnosis[19] and successful experiments have been conducted that tailor medicine to provide cures that work effectively for a specific individual.[20] Experts predict that genomic medicine will become mainstream in the near future.

From a privacy perspective, genomic medicine opens up a new frontier regarding PHI. Genomic information has a unique position among other PHI, as its study leads to the ability to derive more and more information from the same (electronic) DNA sample over time.

Further, disclosure that occurs today will also increase one's vulnerability to future risks that are as yet unknown. As the genomic revolution advances, both the value – and the potential harm – of an individual's genomic data will continue to increase, long after the moment when they were initially sequenced. Within 5 years, expanded sequencing of a person's metagenome, which includes their personal microbiome, will reveal further details of a "genetic fingerprint", encompassing fine-grained information about ethnicity/national origin, places an individual has visited, and even recent contact with other people.[21]

Some other examples of the sensitivity of genomic information include that based on the DNA sample of a person who is five degrees separated from another person, scientists can attribute certain characteristics to the other person. Attribution is not limited to prevalence of certain diseases but extends to behavioral components such as someone's susceptibility to substance abuse, depression, etc.[22] Because of the information that can, or may in the future, be derived from genomic information, in addition to the profits that owning this information may bring, databases with this information have gotten the attention of, and are in large part hosted by, Big Tech companies.[23]

Rise of the illegal trade in PHI

With the advent of more and more connected devices, exposure of cloud platforms, and the sensitive and thus monetary value of PHI, it may come as no surprise that every new year sees more data breaches than the previous.[24] Breached databases are held for ransom and, regardless of ransom paid,

[19] Turro, E., et al. (2020). Whole-Genome Sequencing of Patients with Rare Diseases in a National Health System. Nature 583, 96–102.
[20] https://www.genome.gov/dna-day/15-ways/cancer-genomics, *Using the Genome to Treat Cancer*
[21] F. Briscoe, B. Gray, D. Ferraro, Innovations in medical genomics; what are the privacy and security risks. Penn State University, MARCH 2017.
[22] *Ibid.*
[23] https://www.environmentalmedialab.com/heliotrope/genomics-clouds-by-mel-hogan.
[24] https://healthitsecurity.com/news/over-41.4m-patient-records-breached-in-2019-as-hacking-jumped-49.

are often also sold via the Darkweb[25] or telegram[26]. This results in defamation, fraud, extortion and other harms by cybercriminals.

Currently, HIPMA places obligations on custodians to protect the PHI that they hold. However, there are no real consequences for non-compliance, including where a failure to adequately secure PHI results in a breach. In effect, this creates a negative incentive for custodians to make the investment in proper information security measures to protect PHI. Because investments in information security cost money, and a breach of PHI generally does not, for the purpose of profitability, information security is neglected and any compensating measures for potential harm are at the discretion of the custodian. In late 2019, over two thousand Yukoners were affected by a privacy breach at LifeLabs involving their PHI.[27] The Privacy Commissioner for BC and the Ontario Privacy Commissioner jointly investigated the breach that involved the PHI of millions of Canadians.[28] They found that that LifeLabs failed to implement reasonable safeguards to protect the PHI of its customers.[29]

Evolution of privacy protection in Canada

The privacy law landscape in Canada has changed in recent years. Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) is being reviewed, as is Quebec's private sector privacy law. Quebec is one of three provinces that have private sector privacy laws that are substantially similar to PIPEDA. Alberta and BC are the other two. There are four provinces with health information laws that are substantially similar to PIPEDA. They are New Brunswick, Newfoundland and Labrador, Nova Scotia and Ontario. HIPMA was designed to be substantially similar to PIPEDA, although it has not been designated as such. In order to maintain their substantially similar status, laws declared as such will need to be modified to more closely align with any amendments to PIPEDA or its replacement.

Federal Bill C-11

A summary of Bill C-11, called the *Digital Charter Implementation Act, 2020*, is as follows.

> *On 17 November 2020, the Minister of Innovation, Science and Industry introduced Bill C-11 in the House of Commons. The bill creates two new pieces of legislation: the Consumer Privacy Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act (Tribunal Act). The bill repeals Part 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA) and changes the short title to the Electronic Documents Act.*
> *This is the first bill to fully reform the federal legislation on privacy in the private sector since PIPEDA was adopted in 2000.*

[25] The Darkweb is a collection of websites only reachable via the Onion protocol using a special web browser. The Darkweb has been built to ensure anonymity of both hosts and visitors of these websites and it is used as a digital variant of a black market.
[26] Telegram is a chat client and broadcast channel collection, originating from and broadly used in Russia but also with some 500,000,000 users world-wide.
[27] https://www.yukonombudsman.ca/news/view/111/104.
[28] https://www.cbc.ca/news/canada/british-columbia/lifelabs-data-breach-personal-information-bc-ontario-1.5626985.
[29] *Ibid.*

In general, the CPPA:

- *codifies the contents of the fair information principles set out in Schedule 1 of PIPEDA by rewording them as legislative provisions;*
- *maintains valid consent as the legal basis for the collection, use or disclosure of personal information by an organization (section 15);*
- *includes several exceptions to the requirement for consent, including two new exceptions related to the business activities of an organization and the disclosure of personal information for socially beneficial purposes (sections 18 and 39);*
- *includes the right to erasure (section 55);*
- *incorporates the concept of algorithmic transparency in the form of a right to an explanation concerning decisions made by an automated decision system (sections 62 and 63);*
- *incorporates the concept of data portability by allowing two organizations to disclose personal information between them under a data mobility framework provided under the regulations (section 72);*
- *sets out obligations to de-identify personal information (sections 74 and 75);*
- *grants the Privacy Commissioner (the Commissioner) additional powers, including the ability to make decisions, issue orders and recommend that the new administrative tribunal created by the bill impose a maximum penalty that is the higher of $10,000,000 and 3% of an organization's gross global revenue (sections 92 to 94); and*
- *provides for a maximum fine not exceeding the higher of $25,000,000 and 5% of an organization's gross global revenue in the case of a conviction for contravening certain specific provisions of the CPPA or in the case of obstructing the Commissioner's work (section 125).*

As for the Tribunal Act, it establishes the Personal Information and Data Protection Tribunal (the Tribunal) and defines the internal operation and principles on which its proceedings are founded.

The short title of the bill is the Digital Charter Implementation Act, 2020. Canada's Digital Charter (the Charter) was unveiled by Innovation, Science and Economic Development Canada (ISED) in 2019. The Charter is the result of consultations that began in June 2018 with many stakeholders. The 10 principles set out in the Charter include:

- *control and consent;*
- *transparency, portability and interoperability; and*
- *strong enforcement and real accountability by imposing clear and meaningful penalties for violations of the laws and by adopting regulations that support the principles set out in the Charter.*

After releasing the Charter, ISED issued a discussion paper on PIPEDA reform, outlining issues and possible legislative amendments. The bill appears to stem from those consultations.

The bill responds to several calls for reform, including by the Commissioner and the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee). For example, in his 2018–2019 annual report on privacy law reform, the Commissioner recommended the modernization of federal privacy laws, including PIPEDA. Among other things, he recommended a rights-based approach for protecting the privacy of Canadians, proactive inspection powers without grounds and privacy by design obligations.

In his 2019–2020 annual report on privacy in a pandemic, the Commissioner reasserted the need to reform federal privacy laws, including PIPEDA. He noted that "[t]he law is simply not up to protecting our rights in a digital environment." More recently, he made proposals for regulating artificial intelligence, including suggestions for amending PIPEDA.

The Committee has recommended a number of amendments to be made to PIPEDA in recent years, including in its 2018 report on the review of PIPEDA. Numerous recommendations for modernizing PIPEDA were also made in the two reports the Committee published in 2018 as part of its study of the breach of personal information involving Cambridge Analytica and Facebook.

The bill appears to address some of the past recommendations made by the Commissioner or the Committee, particularly by granting additional powers to the Commissioner, introducing a tougher regime of monetary penalties and incorporating the concepts of data portability and algorithmic transparency into the CPPA.[30]

[headings and citations omitted]

The Privacy Commissioner of Canada issued a statement on November 19, 2020, about Bill C-11. Some of his comments about the bill are as follows.

The Office of the Privacy Commissioner of Canada (OPC) welcomes the recent introduction of Bill C-11, which aims to modernize federal privacy law as it relates to the private sector. This ambitious reform initiative includes several significant improvements. However, the Bill also raises a number of questions about its ability to effectively protect privacy in a constantly evolving digital society.

Among these improvements, we see a complete rewriting of the Act's structure. The old model, which reproduced verbatim an industry code of conduct, is replaced with a clearer, more readable law that sets out rights and obligations rather than recommendations.

The Bill would adopt elements of our Guidelines for obtaining meaningful consent, and would create new transparency requirements for the use of artificial intelligence.

[30] https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/432C11E.

The Bill would give the OPC real order-making powers, rather than the more limited powers proposed in the government's 2019 Digital Charter. However, financial penalties would fall under the responsibility of a new tribunal, which would also be an appeal body for the OPC's decisions. We believe citizens should have access to quick and effective remedies. We are examining whether the addition of a new structure is likely to achieve this result.

That being said, new enforcement powers are only a means, a tool by which to enforce the law. In the case at hand, the primary role of the legislation is to enact standards and rules that effectively protect privacy while permitting and encouraging commercial activities.

We have previously recommended that the law should permit the use of personal information for responsible innovation and socially beneficial uses, which is consistent with the Bill, but within a legal framework that would entrench privacy as a human right and as an essential element for the exercise of other fundamental rights.[31]

[underlining and link in original]

Quebec Bill C-64

A summary of Bill-C-64 is as follows.

*The Act Respecting the Protection of Personal Information in the Private Sector (the "**Private Sector Act**"), adopted more than 25 years ago, was introduced at a time when Quebec was the first jurisdiction in North America to adopt legislation to ensure the protection of personal information. However, subsequent legislation adopted by the federal government and technological advances in recent years have meant that the Private Sector Act is no longer adapted to the current context and, moreover, is not consistent either with Canadian federal laws and equivalent legislation in other provinces, nor with the European Union's General Data Protection Regulation ("**GDPR**"), which seems increasingly to be becoming a de facto international standard of reference.*

*On June 12, 2020, Bill 64, An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information (the "**Bill**") was introduced in the Quebec National Assembly. According to the government, once passed, the Bill will promote transparency, enhance data privacy and strengthen user consent by increasing the responsibility of departments and agencies, private companies and, for the first time ever, political parties. Inspired by what is being implemented in other Canadian jurisdictions and in the European Union, the proposed amendments nevertheless remain a uniquely "made in Quebec" approach to privacy protection.*

[31] The full statement can be found at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/s-d_201119/.

The full harmonization of all privacy legislation in Canada, which many would like to see, has yet to be achieved.

…

Principal Amendments

- *Significant administrative sanctions may be imposed by the Commission d'accès à l'information ("**CAI**") of up to $10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions of up to $25 million or 4% of worldwide turnover.*
- *The possibility for a company to be sued for damages.*
- *The requirement to appoint a Chief Privacy Officer and establish governance policies and practices.*
- *New obligations when a data breach incident occurs.*
- *New rights for individuals with regard to data portability, the right to be forgotten and the right to object to automated processing of their personal information.*
- *The creation of an exception allowing the disclosure of personal information in the course of a business transaction without the prior consent of the individuals concerned.*
- *The removal for businesses of the possibility of communicating, without the consent of the persons concerned, nominative lists and new rules governing the use of personal information for commercial or philanthropic prospecting purposes.*
- *The obligation for companies to ensure that pre-established settings for their technology products and services ensure the highest levels of confidentiality by default. (privacy by design).*[32]

[bolding in original and citations omitted]

Other laws relevant to the protection of PI in Canada and the US

Genetic privacy protection legislation

Over the past two decades, several acts have been brought into force to protect against the impact of our relatively recent capacity to analyse the human genome.[33] This process has been improved and commercialized to the point that anyone can get their DNA sequenced for around one hundred dollars by companies such as *23andme, AncestryDNA* and *Family TreeDNA.* These organizations collect the DNA of anyone who wants their service and provide the individual with some information regarding ancestry. The sequencing data received by an individual who utilizes these services can also be uploaded to third parties to learn about prevalence of diseases such as Alzheimers as a result of the individual's genetic coding.

Lawmakers have recognized the discriminatory impact that the results of DNA tests may have and have prohibited discrimination based on DNA. In Canada this was codified in 2017 in the *Genetic Non-*

[32] https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business.
[33] https://www.britannica.com/event/Human-Genome-Project.

discrimination Act (GNA). Although the Act offers blanket protection against any form of discrimination based on someone's genetic makeup, it does not provide any protection of privacy regarding the specific risks of genetic information.[34] California recently enacted the *Genetic Information Privacy Act* (GIPA) which makes a start with protecting this information against adverse effects of its collection by DNA sequencing companies such as those mentioned above, and tech giants who are also putting much endeavour into obtaining this treasure trove of data for monetization.

Patriot Act, CLOUD Act and proposed EARNIT and LAED acts

Certain laws of the USA have an impact on operations of the Yukon's healthcare providers. The *Patriot Act* and the *CLOUD Ac*t effectively require any subsidiaries of US companies to hand over PI in their custody or control if asked to do so by US authorities. The impact is that even if data is stored in Canadian data centres owned by a US company (for example, Amazon or Microsoft Canada, either directly or through subsidiaries), this data including PHI can make its way to the US government.

The LAED[35] and EARNIT[36] proposals that, at the time of writing these comments, were before subcommittees of the US Congress pose another risk for PHI hosted or transmitted by US companies, as both Acts have the potential to weaken encryption of data during transport.

HIPMA next generation

Those responsible for amending HIPMA during its review should take into account the current legal landscape that is evolving, along with new risks to privacy as a result of emerging innovations and developments, and consider what is necessary in this environment to adequately protect PHI in the digital age. Amendments to HIPMA must be forward-thinking to ensure the framework that is designed will ensure that HIPMA's purposes will be achieved.

The Yukon government and custodians are already using technology to improve the delivery of health care services. I anticipate this use will increase and will include the use of AI to enhance or improve the delivery of health care to Yukoners. As indicated above, there are some benefits to such use. However, proper controls will need to be in place to authorize the use and to protect individuals from the harms that may flow from the use of technology to provide health care. Above, we referenced some legal frameworks under review in Canada that are designed to protect privacy in the digital age. There are many other jurisdictions that are developing similar frameworks that may be worth examining.

Facilitating innovation in healthcare cannot be achieved in a responsible manner without considering the privacy rights of individuals. The choice of controls that authorize innovation must take into account these rights and be designed to preserve privacy rights in that environment.

[34] Also see the chapter on genomic medicine.
[35] https://www.congress.gov/bill/116th-congress/senate-bill/4051/.
[36] https://www.congress.gov/bill/116th-congress/senate-bill/3398/text.

Recommendation 1

To ensure the Yukon's custodians are able to innovate in the delivery of health care by drawing on scientific and technological advances in health care delivery, it is recommended that HIPMA be amended to facilitate this innovation, taking into account the following:

- **(a) the social and environmental developments evolving as a result of the pandemic that have had and will continue to have a significant impact on the ability of individuals to meaningfully control their PHI;**
- **(b) the impact on the health system that will emerge as a result of aging populations;**
- **(c) the digital transformation that will impact how health care is delivered;**
- **(d) advances in personalized medicine;**
- **(e) the risks to privacy in this environment including from the emergence of the illegal trade in PHI and from foreign actors; and**
- **(f) the modernization of privacy laws in Canada and internationally to address the risks to privacy stemming from the digital environment wherein PHI is being processed.**

Oversight powers need to be strengthened to facilitate innovation in health care delivery

To adequately protect the privacy rights of Yukoners in this environment, the authority granted to custodians to innovate in health care delivery must be balanced with controls that facilitate compliance, including strong oversight.

Strong oversight requires that the IPC be given adequate power to protect individuals from harms flowing from non-compliance.

In his 2018-2019 Annual Report to Parliament on the *Privacy Act* and PIPEDA,[37] the Privacy Commissioner of Canada, Daniel Therrien, stated the following about the need for the Privacy Commissioner of Canada to be given order-making powers as the digital economy in Canada evolves and the use of technology to process large amounts of personal information is ubiquitous. His comments illustrate that order-making powers are necessary to facilitate consumer trust in the digital economy and increase participation.

> *Fourth and finally, the law should provide for enforcement mechanisms that ensure individuals have access to a quick and effective remedy for the protection of their privacy rights, and that*

[37] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.

create incentives for broad compliance at all times by federal institutions and commercial organizations.

Canada's laws have unfortunately fallen significantly behind those of trading partners in terms of the enforcement of privacy laws. At the same time, most Canadians believe their privacy rights are not respected by organizations. This is a damning condemnation, and, in my view, an untenable situation in a country governed by the rule of law. It is certainly not conducive to building consumer trust, one of the government's stated objectives.

The government's Digital Charter suggests that my Office should be granted "circumscribed" order-making powers and that before fines are imposed for violations of the law, I have identified following an investigation, I should first convince the Attorney General to further investigate and eventually bring the matter before a judge. By contrast, my EU and US equivalents, among others, can directly order companies to comply with the law and can order sizeable fines, subject of course to judicial review. In my view, the government's proposal is very inefficient, given it would seriously delay the enjoyment of rights by individuals to several years after they have filed a complaint. Justice delayed is justice denied.

True order-making powers and fines would change the dynamic of our discussions with companies during investigations, leading to quicker resolutions for Canadians. At the moment, as we saw in our Facebook investigation, an organization that we have found in contravention of the law can simply ignore our recommendations and "wait it out" until the courts have come to the same conclusion as my Office. In the government's proposal under the Digital Charter, a further step would be added, in the form of a review by the Attorney General.

Both the current framework and the government's proposal create an excellent incentive for companies not to take privacy seriously, change their practices only if forced to after years of litigation, and generally proceed without much concern for compliance with privacy laws. My fellow privacy commissioners at both the provincial and international levels who have already been empowered to make orders and impose fines report that these enforcement tools have led to much more cooperation from companies. When the regulator finds a violation, companies are more willing to correct deficiencies, without long delays.

Ultimately, enforcement mechanisms should result in quick and effective remedies for individuals, and broad and ongoing compliance by organizations and institutions. Only then will trust in the digital practices of companies and government reach the levels we all want.

In a joint resolution issued by Canada's privacy commissioners in October of 2019,[38] they urged their respective governments to, *inter alia,* improve enforcement measures. The measures are identified in the resolution as follows.

[38] https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/.

With respect to enforcement:

- *Individuals have effective means to assert their access and privacy rights and to challenge entities' compliance with their legislated obligations;*
- *Effective independent oversight offices are sufficiently funded and can rely on extensive and appropriate enforcement powers adapted to the digital environment, such as the power to conduct own-motion investigations and audits, the power to compel records and witnesses as necessary for reviews and investigations, the power to issue orders, and the power to impose penalties, fines or sanctions;*
- *Commissioners are consulted on changes to legislation that impact access to information or privacy rights.*

The context provided in the resolution in support of the need for increased enforcement is as follows.

> *Privacy and access to information are quasi-constitutional rights that are fundamental to individual self-determination, democracy and good government. New technologies have numerous potential benefits for society, but they have impacted fundamental democratic principles and human rights, including privacy, access to information, freedom of expression and electoral processes.*
>
> *Increasingly, the public is concerned about the use and exploitation of personal information by both governments and private businesses and, in particular, the opaqueness of information handling practices. Security breaches are happening more often and have impacted millions of citizens.*
>
> *While it is important to acknowledge that there have been legislative advances made in some Canadian jurisdictions, there is still ongoing work required to enhance and establish consistent modernization. Most Canadian access and privacy laws have not been fundamentally changed since their passage, some more than 35 years ago. They have sadly fallen behind the laws of many other countries in the level of privacy protection provided to citizens.*

In my 2019 Annual Report of the IPC,[39] I stated that:

> *HIPMA is scheduled for review in 2020 and I intend to recommend that the IPC be granted "own motion" authority under that law as well. I am also planning to recommend that the IPC be given order-making powers under the new version of HIPMA that are enforceable by the courts, together with enforceable notices to produce. Discussion about the need to increase the powers of IPCs is occurring across Canada. The discussion centres on the need to ensure compliance with access to information and privacy laws, given the massive data breaches that are occurring and the diminishing trust of Canadians in the ability of organizations, including government, to*

[39] https://www.yukonombudsman.ca/uploads/media/5f1b6864e6790/YK%202019%20Annual%20Report_Web%20July%2022%202020.pdf?v1, at pp. 27 and 28.

> *adequately protect their personal information. Another impetus for these changes is to build trust amongst Canadians in support of a burgeoning digital economy…*

In reference to a Government of Canada publication "Enhancing Enforcement and Oversight in Strengthening Privacy of the Digital Age", I quoted the following from the publication:

> *There is a growing view that the ombudsman model and enforcement of PIPEDA, which relies largely on recommendations, naming of organizations in the public interest, and recourse to the Federal Court, to effect compliance with privacy laws, is outdated and does not incentivize compliance, especially when compared to the latest generation of privacy laws. The current state of affairs cannot continue; meaningful but reasoned enforcement is required to ensure that there are real consequences when the law is not followed.*

I highlighted that "[t]he recommendations in the document referenced above are to increase the powers of Canada's Privacy Commissioner in PIPEDA, by giving the Commissioner, among other things, the power to issue binding orders. As indicated, HIPMA was written to be substantially similar to PIPEDA, which is the privacy law referenced in the foregoing document".

In closing I stated that:

> *In order to protect and preserve Yukoners' rights under these laws, the IPC must be given sufficient authority to ensure that public bodies and custodians are complying with the ATIPP Act and HIPMA. In my view, the time has come to increase the powers of the IPC in Yukon in order to achieve this objective.*

The digital transformation has had a significant impact on individuals' privacy rights. The complex nature of data processing today, including through the use of AI, is a game changer. Today vast amounts of PHI are being processed by health care providers in an environment that is extremely complex and opaque. It is no longer reasonable in this environment to leave it up to individuals to fight for their rights in court as in doing so they would be at a significant disadvantage in trying to advance their case with limited knowledge about this complex environment.

Custodians are now choosing to use technological advancements to deliver health care services for obvious reasons. The pandemic has led to a significant surge in the use of technology to deliver health care services. It is only a matter of time before AI is used as part of service delivery.

Investigations into non-compliance require significant expertise in understanding not only the law, but also the environment in which data is processed. IPCs in Canada were established to provide individuals with a remedy to resolve disputes about compliance without involvement of the court. These offices have significant expertise in evaluating compliance in a complex technological environment.

In HIPMA, the IPC has only the power to recommend to remedy non-compliance. If refused, it is up to an individual to go to court and fight for their privacy rights. A scan of health information privacy laws in Canada shows that most have remedial models that do not leave the issue of non-compliance and a refusal to accept an IPC recommendation in the hands of an individual whose privacy rights were found

to have been violated.

There are 10 provinces/territories in Canada with health information legislation. Of the 10, four have order-making power. The remaining six have recommendation remedial authority. Manitoba's Ombudsman can refer a matter to an adjudicator if a custodian refuses her recommendations. In Newfoundland/Labrador and the NWT, IPCs can appeal a decision to the court if a custodian refuses their recommendations. There are only three jurisdictions where it is up to the individual to appeal a decision by a custodian to refuse an IPC's recommendations. These three laws (in Saskatchewan, Nova Scotia and New Brunswick) went into effect more than a decade ago and have not been substantially amended. As indicated, the BC IPC has order-making powers in regard to decisions made by public and private sector health care providers. Nunavut only has recommendation remedial authority over public health care bodies and the individual may appeal a refusal by a public body to accept the IPC's recommendations. Nunavut's ATIPPA went into effect in 1996 with minor amendments.

Given this context, the time has come to provide the Yukon IPC with order-making power. Where a custodian disagrees with the IPC's decision, they can seek judicial review of the decision. The custodian is in a much better position to advance their arguments of compliance given that they have detailed knowledge about how their data is processed. Additionally, as was recognized by my colleagues in Canada, order-making power is now the norm in modern privacy laws and a necessary component of facilitating compliance in the digital environment.

In terms of the IPC's other powers under HIPMA, they should at minimum align with those in the new ATIPP Act.

In Yukon, our *Access to Information and Protection of Privacy Act* was replaced with a new more modern version that takes into account the use of technology for innovation by public bodies. It went into effect in April of 2021.

Access to Information and Protection of Privacy Act (2018)

The new *Access to Information and Protection of Privacy Act* (ATIPPA) is a relatively modern piece of privacy legislation that was designed to facilitate the use of technology to process personal information. It authorizes public bodies to collect, use and disclose personal information for identity management, for integrated programs and activities of public bodies, and for data-linking. There are detailed processes for undertaking these activities including that the public body is required to submit privacy impact assessments and security threat risk assessments to the IPC and consider and respond to her comments prior to the start of any of these activities. The ATIPPA regulations contain detailed information security requirements and the Act, together with the regulation, require the implementation of a privacy and security information management program and mandatory breach recording and reporting by all public bodies. In recognition of the expanded authority and measures designed to mitigate the risks to privacy, the IPC's authority was expanded to ensure more effective oversight. The IPC now has own motion authority and can conduct compliance audits. Her powers of investigation were also expanded. Included among them is that she has the same power as vested in a

court to compel testimony or documentary evidence and she has the power of entry and to converse with any person in private.

The need for own motion authority has proven necessary. In HIPMA, the IPC has authority to issue comments and advice on matters of privacy protection to facilitate compliance with the Act and to make recommendations with regard to the Act. Experience has demonstrated that recommendations made as part of these compliance review activities have largely been ignored. There have been occasions where we found non-compliance when reviewing PIAs which goes unanswered. Without the ability to conduct own motion investigations, there is little the IPC can do when this occurs.

Another important factor supporting the need for own motion authority is in regard to investigations of offences. On occasion, during investigation or when conducting compliance review activities, we have seen potential offences. Without the ability for the IPC to commence an offence investigation, she cannot investigate if an offence has occurred. Therefore, she must have own motion authority. Without this authority, it renders the offence provisions in HIPMA essentially meaningless.

Scope of investigation for non-compliance needs to be expanded

Lastly, the scope of investigation for non-compliance with HIPMA's requirements needs to be expanded. Currently, any person may make a complaint about a *custodian's* potential non-compliance and the IPC may investigate. There are provisions in HIPMA that apply to persons other than custodians. For example, no "person" is authorized to collect, use or disclose an individual's public health insurance plan number or card. No "person" is authorized to access the YHIN unless authorized. Having the ability to investigate alleged unauthorized access to YHIN will be particularly important given the implementation of the 1Health system that is currently being launched in the Yukon. The meaning of "person" in HIPMA is non-exhaustive. To make these provisions meaningful, the IPC must have the authority to investigate any suspected non-compliance with HIPMA by any person, including an agent who also has obligations under HIPMA that are distinct from a custodian's. I will note here that in subsection 7 (1) it identifies that the Act applies to:

> *(a) the collection, use and disclosure of personal health information by*
> *(i) the Minister or the Department, or*
> *(ii) any other custodian, if the collection, use or disclosure is undertaken for the purpose of providing health care, the planning and management of the health system or research;*
> *(b) the collection, use or disclosure by any person of a Yukon public health insurance plan number; and*
> *(c) a request made by any person for the production of a YHCIP card.*

This provision should be evaluated to ensure all those subject to the Act by virtue of their obligations thereunder or in regard to its prohibitions are captured within this provision.

Recommendation 2

To ensure Yukoners' privacy rights will be protected in an environment where their PHI is processed through the use of technology designed to enhance health care delivery, it is recommended that the IPC be given the following powers:

- **(a) order-making power to remedy *any* non-compliance with HIPMA, or in the alternative the power to defer a refusal by a custodian to accept a recommendation to an adjudicator who has order-making power or the power to take a custodian to court if they refuse a recommendation;**
- **(b) the same powers of a board of inquiry under the *Public Inquiries Act*;**
- **(c) power to investigate *any* suspected violation of HIPMA on the IPC's own motion;**
- **(d) power to conduct compliance audits;**
- **(e) expanded investigative powers that apply to investigations and audits that include:**
    - **i. the same power as is vested in the court to summon a person to appear before the IPC;**
    - **ii. the same power as is vested in a court to compel a person summoned to give oral or written testimony;**
    - **iii. the same power as is vested in a court to compel a person to produce to the IPC information or a record that in the opinion of the IPC is relevant to the investigation;**
    - **iv. the same power as is vested in the court to examine information or a record that is produced to the IPC;**
    - **v. power to enter any premises occupied by a custodian on satisfying any security requirements of the custodian relating to the premises;**
    - **vi. power to converse in private with any person in the custodian's premises;**
    - **vii. power to conduct interviews with any person that the IPC reasonably believes may know or hold information that is relevant to an investigation;**
    - **viii. power to receive and consider evidence of any other type that in the opinion of the IPC may be relevant to the investigation or audit, whether or not the evidence would be admissible in a proceeding before a court;**
    - **ix. in respect of a matter under investigation, the power to determine each question of fact and law arising in relation to the matter;**
    - **x. power to join two or more complaints related to the same or similar matters for the purpose of conducting a single investigation into the complaints; and**
    - **xi. power to administer oaths.**

Recommendation 3

I recommend that the scope of application of HIPMA in section 7 be evaluated to ensure all those subject to the Act by virtue of their obligations thereunder or in regard to its prohibitions are captured within this provision.

Substantial similarity between HIPMA and PIPEDA

Unlike in other jurisdictions,[40] HIPMA has not been declared substantially similar to PIPEDA, even though it was designed with that purpose in mind. For this status to be granted, the Yukon government would need to apply to Industry Canada, which is responsible for reviewing applications to determine if a provincial or territorial law meets the criteria for substantial similarity to PIPEDA. To my knowledge, this process has not been initiated.[41] Without this status, an unnecessary burden is placed on private sector custodians as they have to fulfill the obligations of both Acts. Private sector custodians must know and apply the provisions of both Acts to their operations which creates overlap that may cause confusion. For example, a private sector custodian must in certain and somewhat different circumstances report privacy breaches to both the Office of the Privacy Commissioner of Canada (OPC) and to the Yukon's IPC. As indicated, PIPEDA is currently under review (see the proposed Bill C-11[42]) and from preliminary information about the review as noted herein, it is clear that the revised PIPEDA will have a lot more requirements for anyone subject to that Act. If the goal is for HIPMA to be declared substantially similar to PIPEDA or its successor legislation, it will need to be updated to reflect these changes. It would be in the best interests of private sector custodians if HIPMA is declared substantially similar to PIPEDA or its successor legislation, in order to reduce the regulatory burden for these custodians and help provide clarity on compliance criteria.

Recommendation 4

To alleviate the pressures on private sector custodians to comply with multiple privacy laws, I recommend that the Yukon government seek to have HIPMA declared substantially similar to PIPEDA or its successor legislation.

[40] The health privacy laws in New Brunswick, Newfoundland and Labrador, Nova Scotia and Ontario have been declared substantially similar to PIPEDA.
[41] The process to obtain substantially similar status is set out at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/legislation/leg-rp_030611/.
[42] https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

Additional considerations regarding HIPMA-specific provisions

HIPMA has been in effect for five years now and our experience with the Act has demonstrated some issues that should be addressed.

Application of HIPMA to social services records

HIPMA's purposes provisions make it clear that the law is intended to protect the privacy of PHI that is collected, used, disclosed, accessed or managed in the delivery of health care and to manage the Yukon's publicly-run health system. It is not intended to apply, and should not apply, to social services records in the custody or control of the Department of Health and Social Services. There is simply nothing in HIPMA to suggest otherwise.

The only reason that HIPMA applies to social services records is because the definition of PHI includes 'registration information'. In the *Health Information General Regulation*,[43] "registration information" of an individual means the individual's name, gender, date of birth, date of death, residential address, telephone number, email address, and personal health number issued by a province or Canada. The meaning of 'registration information' together with the mixed record rule in section 10 and the application of HIPMA to the collection, use and disclosure of PHI by the "Minister or the Department" in paragraph 7 (1)(a)(i), means that any registration information that is mixed in a record with an individual's PI (as defined in ATIPPA), becomes PHI that is governed by HIPMA instead of ATIPPA.

No other jurisdiction in Canada that I am aware of has government social services records that are subject to health information legislation for the obvious reason that these records do not contain health information. These records should be subject to ATIPPA, not HIPMA.

Recommendation 5

To provide Yukoners with the right to access social service records under public sector privacy law as is the case in every other jurisdiction in Canada, I recommend that HIPMA be revised to remove the application of HIPMA to social services records that are collected by or that are in the custody and control of the Department of Health and Social Services.

Authority for a public body custodian to collect PHI for a program or activity

In the second consideration report that I issued under HIPMA, I came across an issue that I highlighted. As indicated, HIPMA was designed to be substantially similar to PIPEDA. PIPEDA is consent-based legislation. What this means is that consent is the primary means to collect, use and disclose PI and is the means by which individuals exercise control over their PHI.

[43] O.I.C. 2016/159.

When HIPMA was enacted, a provision that does not exist in other health information laws was included. This provision authorizes a public body-custodian to collect PHI if "the collection relates to and is necessary for carrying out a program or activity of a public body or a health care program or activity of a custodian that is a branch, operation or program of a Yukon First Nation." Not only is this provision inconsistent with the consent-based nature of HIPMA, but it is also highly problematic from a control perspective. In recognition of the issue, I stated the following about the provision.

> *HIPMA is consent based legislation. The purpose for this is clear. Consent is the primary way that individuals are able to control their own personal health information. When custodians do not seek consent, individuals may lose their ability to exercise any control.*
>
> *Unfortunately, in HIPMA there is authority for public body custodians to not only use and disclose personal health information for the provision of health care without consent but to also collect it without consent. Subsection 53 (c) authorizes a custodian who is a public body to collect personal health information without consent.*[44] *"Public body" is defined in section 2 of HIPMA as having "the same meaning as in the Access to Information and Protection of Privacy Act" (ATIPP Act). The result of this provision is that the two largest custodians in Yukon,* [Yukon Hospital Corporation] *and* [the Department]*, are not required to obtain an individual's consent to collect their personal health information. HIPMA differs from other similar health information legislation in Canada that is based on the Model Code in this regard.*
>
> *Not only is this authority contrary to the Model Code requirement for consent, but it also has significant consequences as it pertains to an individual's ability to exercise control over their personal health information. If these custodians elect to use this authority, individuals' ability to control their personal health information through the consent provisions is, essentially, removed. In my view, the broad authority of these custodians to collect, use and disclose personal health information without consent disadvantages Yukoners. When HIPMA is reviewed, I intend to recommend that this authority be removed. Details about this authority follows.*
>
> *Consent and Control in HIPMA*
>
> *In HIPMA, custodians may obtain consent in one of two ways, either expressly or impliedly. Custodians can meet the requirements of implied consent simply by posting a notice containing specific wording. As stated, for consent to be valid under HIPMA, it must be knowledgeable. Consent is knowledgeable only if the individual knows:*
>
> *a. the purpose of the collection, use or disclosure;*

[44] *There are three ways a custodian can collect personal health information in HIPMA. They are set out in section 53. This section authorizes a custodian to collect an individual's personal health information only if (a) the custodian has the individual's consent and the collection is reasonably necessary for a lawful purpose; (b) the collection is authorized by law; or (c) the collection relates to and is necessary for carrying out a program or activity of a public body or a health care program or activity of a custodian that is a branch, operation or program of a Yukon First Nation.*

b. that they may give or withhold consent and having once given consent, may withdraw that consent; and

c. that without their consent the personal health information can be collected, used or disclosed only in accordance with HIPMA.

The reason that consent must be knowledgeable is obvious. It informs individuals about what a custodian may do concerning their personal health information; it informs them about how they exercise control over it; and it informs them that there are limits to this control as set out in HIPMA. The key is that individuals are informed.

When a custodian does not obtain consent from an individual to collect, use or disclose their personal health information, the individual is left uninformed about their choices. Individuals who do not give their consent, express or implied to the collection of their personal health information are never informed about the purpose of the collection or that they can refuse consent. Without this information, they do not know they have any choice about what happens with their personal health information when engaging the services of these custodians.

Even if a public body custodian only obtained consent for the collection of personal health information from individuals and did not do so for its use or disclosure, while not perfect, individuals would at least be aware at the point of collection that they have some ability to control their own personal health information. This may then prompt them to ask questions about its subsequent use or disclosure.

As it stands, in HIPMA if a public body custodian does not obtain consent to collect personal health information by relying on subsection 53 (c) and also does not obtain consent for its use under paragraph 55 (1)(a) or disclosure under subsection 58 (a), the individual is left completely in the dark about their choices and their ability to exercise the control afforded to them by HIPMA over their personal health information.

As can be seen by comparing HIPMA with other health information privacy legislation in Canada that is based on the Model Code, HIPMA is different because it allows public body custodians to collect personal health information without consent.

Health Information Privacy Laws in other Jurisdictions

New Brunswick's Personal Health Information Privacy and Access Act, SNB2009, c P-7.05 (NB PHIPAA)

Individuals whose personal health information is collected by custodians subject to NB PHIPAA are informed about the collection of their personal health information in one of two ways. Either they are informed when they are asked for consent by a custodian or, where no consent is sought, they are informed by way of notice.

The general rule in NB PHIPAA is that custodians are required to obtain consent to collect personal health information from an individual. Consent must be knowledgeable. The knowledgeable requirement includes ensuring that they are informed that they can refuse or withdraw consent. The only other ways a custodian can collect personal health information are as follows:

> *a. the individual is incapable of giving consent and there is no substitute decision maker, or they have been certified under the Mental Health Act or it is necessary to provide health care to the individual;*
>
> *b. if [NB PHIPAA] requires or permits it; or*
>
> *c. they are collecting for an integrated service, program or activity.*[45]

For any collection of personal health information with or without consent, a custodian is required to "before it is collected or as soon as practicable afterwards to take reasonable steps to inform the individual of the purpose of collection..." The exception to this rule is if the custodian, through its consent process or otherwise, has already informed the individual of the purpose. The process of being informed through consent or notice, as the case may be, provides an individual with choices about collection. This may, in turn, signal to them that they also have choices for use and disclosure

Newfoundland and Labrador's Personal Health Information Act, SNL 2008, c P-7.01 (NL PHIA)

In NL PHIA, individuals are informed about the collection of their personal health information through the consent requirements.

The general rule is that a custodian is required to obtain consent to collect personal health information from an individual. The exception is where the individual is incapable of providing consent and:

a. there is no representative or one available in a timely manner to give consent;

b. the individual is certified under the Mental Health Act;

c. the collection is necessary to provide health care to the individual.[46]

Consent must be knowledgeable. The knowledgeable requirement includes ensuring that they are informed that they "may give or withhold consent". Under NL PHIA, individuals have the

[45] "Integrated service, program or activity" is defined in New Brunswick's *Right to Information and Protection of Privacy Act* as " an authorized service, program or activity that provides support or assistance with respect to the mental, physical or social well-being of individuals through (a) a public body and one or more other public bodies working cooperatively, or (b) one public body working on behalf of one or more other public bodies".

[46] NL PHIA paragraph 29 (1)(a).

same authority as under NB PHIPAA to refuse to give consent, place conditions on it or withdraw it after it is given.

Ontario's Personal Health Information Protection Act, 2004, SO 2004, c 3 Sch A (ON PHIPA)

In ON PHIPA, individuals are informed about the collection, use and disclosure of their personal health information through the consent requirements. The general rule in ON PHIPA is that custodians are required to obtain consent for the collection, use or disclosure of personal health information.

Consent must be knowledgeable.

Consent is knowledgeable if the individual knows the purpose of collection, use or disclosure and that they may give or withhold consent. Despite the general rule, custodians are authorized to collect personal health information if the information is reasonably necessary to provide health care to the individual and it is not reasonably possible to obtain consent in a timely manner.

Authority of Public Bodies in HIPMA

The addition of subsection 53 (c) in HIPMA, which authorizes public body custodians to collect personal health information without consent and additionally to use and disclose it without consent to provide health care means that, other than what may be obvious to the individual at the point of collection, and during any interactions with health care providers while receiving care, the individual may never know why their personal health information is being collected and used, or to whom it will be disclosed.

Unlike NB PHIPAA, HIPMA does not contain any notice requirements outside the consent rules that require custodians to provide information to individuals about the purpose of collection and their rights.

Prior to HIPMA, these public bodies were required under the ATIPP Act to inform individuals about the purpose of collecting personal health information along with the contact information of an individual who could answer questions. The addition of subsection 53 (c) in HIPMA, without adding a notice requirement, has the effect of allowing public body custodians to collect personal health information without providing any information to individuals about the collection. This potentially removes the only means of informing individuals about their rights.

As a result of the foregoing, in my view subsection 53 (c) should be removed from HIPMA so an individual's ability to control their personal health information through the consent provisions is not compromised because of this subsection.

Recommendation 6

To ensure individuals can exercise effective control of their PHI, it is recommended that:

- **(a) the authority of a public body custodian to collect PHI without consent be removed from HIPMA; or**
- **(b) if this authority remains, it is recommended that custodians who exercise this authority be required to provide notice to the individual about the collection, which notice must at minimum include:**
  - **i. the purpose of the collection;**
  - **ii. the authority for collection;**
  - **iii. that the PHI is being collected without consent;**
  - **iv. the right to refuse the collection;**
  - **v. the name and contact information of the custodian's contact individual to exercise their right of refusal or to answer any questions about the collection and right of refusal; and**
  - **vi. information about how to make a complaint to the IPC if the individual believes that the collection is not authorized.**

Requirements of custodians to transfer records to a successor custodian after ceasing operations

The successor provisions under HIPMA are ineffective in practice. To date there have been four instances of custodians closing their practices and records not being transferred in accordance with the successor provisions in HIPMA. In one case, a dentist-custodian left the territory and left health records behind in an abandoned office. Despite our best efforts, we could not locate the custodian. In this case, the Minister exercised her authority to transfer the records. They were transferred to the Department of Health and Social Services (Department). I was informed of another similar case, but not the specifics. In 2019, Many Rivers Society closed its doors and failed to transfer their patient records. The records were collected by the Department. The Department and the IPC disagreed on the legal authority for the Department's acquisition of the records and the dispute was never resolved. Again in 2019, a psychiatrist-custodian left the Yukon, and the records allegedly were not transferred. At the time of writing these comments, we are in consideration on the matter and therefore, cannot comment further.

These successor provisions were added into health information laws in Canada to protect PHI when custodians cease practice. Prior to these provisions, there were occasions when custodians closed their practice, did not transfer their records, and failed to dispose of or store them properly, leading to privacy breaches and loss of patient PHI. These provisions were designed to ensure that when a custodian ceases operations, PHI of patients is transferred to a custodian who will continue to provide care and ensure their protection if not transferred. They were also designed to provide certainty to

individuals about the location of their PHI post-closure and ensure ongoing access until the records are securely destroyed according to the custodian's retention period.

What has occurred reveals some significant shortcomings in the current model under HIPMA as it relates to these provisions that need to be addressed.

Current model

Deemed custodians

3(1) If at any time a person would, but for this subsection, cease to be a custodian, and immediately before that time the person had the custody or control of personal health information, the person is deemed for the purposes of this Act to remain a custodian with respect to that personal health information while the person has its custody or control.

(2) If a custodian who is an individual becomes incapable of managing their affairs or dies, the custodian's guardian or personal representative, as the case may be, is deemed for the purposes of this Act to be a custodian with respect to any personal health information contained in a record that is, or that but for the custodian's death or incapacity would be, in the custody or control of the custodian.

(3) If a custodian that is not an individual is bankrupt or insolvent or is liquidated, dissolved or wound up, any person who, as a result of the bankruptcy, insolvency, liquidation, dissolution or winding-up, obtains the custody or control of records that contain personal health information is deemed to be a custodian with respect to that personal health information. S.Y.2013, c.16, s.3

Continuing duties of a custodian

23(1) The duties imposed under this Act on a custodian with respect to personal health information, and records containing personal health information, in the custody or control of the custodian apply to the custodian until the custodian transfers custody and control of the personal health information or the records to a successor of the custodian in accordance with section 60 or to a prescribed person in accordance with the prescribed requirements, if any.

(2) If a custodian fails to carry out their duties under this Act, the Minister may, with the prior consent of the person to be appointed, appoint a person to carry out those duties in place of the custodian until custody and control of the personal health information or of the records are transferred to a successor of the custodian in accordance with section 60 or to a prescribed person in accordance with the prescribed requirements, if any.

(3) An appointment under subsection (2) may be made subject to any terms and conditions that the Minister considers appropriate in the circumstances.

(4) The Minister may require a custodian who fails to carry out their duties under this Act

(a) to reimburse the Government of Yukon for any costs it reasonably incurs as a result of the

custodian's failure; and

(b) to pay a person appointed under subsection.

(2) to carry out the custodian's duties an amount determined by the Minister, as compensation for the person's services under that subsection, and to reimburse the person for any disbursements it reasonably makes in providing the services. S.Y.2013, c.16, s.23

Disclosure to successor

60(1) In this section

"potential successor" of a particular custodian means a person who

(a) contemplates entering into an agreement with the particular custodian under which the particular custodian will relinquish to the person the custody and control of personal health information, and

(b) is a custodian or can reasonably be expected, if it enters into the agreement described in paragraph(a), to become a custodian;

"successor" of a particular custodian means another custodian to whom the particular custodian has, under an agreement between them, relinquished the custody and control of personal health information.

(2) A custodian may, without an individual's consent, disclose the individual's personal health information to a potential successor of the custodian for the purpose of allowing the potential successor to assess and evaluate the operations of the custodian, if the potential successor first enters into an agreement with the custodian to keep the personal health information confidential and secure and not to retain it longer than is necessary for the purpose of the assessment or evaluation.

(3) A custodian may transfer a record of an individual's personal health information to the custodian's successor unless the individual expressly instructs the custodian not to make the transfer.

(4) If, under subsection (3), a custodian transfers a record of an individual's personal health information to the custodian's successor and an instruction of the individual prevents the custodian from transferring all the individual's personal health information that the custodian has reasonable grounds to believe is necessary for the provision of health care to the individual, the custodian must notify the successor of that fact.

(5) A custodian must make reasonable efforts to give notice to an individual before transferring a record of the individual's personal health information to the custodian's successor or, if that is not reasonably possible, as soon as possible after transferring the record. S.Y.2013, c.16, s.60

The remedy for abandoned records in Saskatchewan

In 2014, in response to concerns associated with the abandonment of records by health care providers in Saskatchewan, a working group (WG)[47] was formed by Saskatchewan's Ministry of Health to examine the issue and make recommendations. The WG examined the provisions of Saskatchewan's *Health Information Protection Act* (HIPA) that pertain to the transfer of records by a trustee when they cease practice.[48] The WG issued the Health Records Protection Report in April of 2014 (Report).[49] The WG's mandate was:

> *(i) to examine and provide advice on the mechanisms for enforcement of trustee responsibilities to protect patient records as required under HIPA. The Working Group will review not only the current enforcement mechanisms, but also comment on specific changes which may be desired to clarify trustee responsibilities or to assist in achieving trustee compliance with HIPA; and*
>
> *(ii) to examine and recommend specific changes which will prevent abandonment of patient records, thereby protecting patient confidentiality and reducing events requiring need for enforcement.*[50]

The WG described the "abandoned records problem" as follows.

> *The Working Group discussed the challenge associated with dealing with records that are found abandoned, including taking control of those records and finding appropriate repositories so that personal health information can be available to patients but still remain secure. The group noted that, while there should not be a circumstance where records are found abandoned, such incidents continue to occur notwithstanding the clear responsibilities trustees have to protect those records. While human error can occur, the number of cases where records are found to be improperly stored or destroyed is troubling and indicates that there may be a lack of education, understanding and clear procedure in place within some trustee operations. In addition, there are a variety of circumstances including death, retirement, change of practice or relocation of a trustee which if not properly handled, can expose patient medical records to privacy and security risks. While HIPA contemplates that there should be designated archives where trustees can deliver patient records for storage when they cease to practice, this system has not proven to be effective. Therefore, the Working Group concluded that changes should be made to develop a more effective records repository solution, which would assist in preventing abandoned records, and be available to maintain records which might be found abandoned. This solution, however, is not intended to negate the trustee's obligations with respect to records management, nor is it*

[47] The working group had representatives from the Ministry of Health, Ministry of Justice and Attorney General, Saskatchewan College of Physicians and Surgeons, Saskatchewan Registered Nurses Association, Saskatchewan College of Pharmacists, Saskatchewan Medical Association and the Patient Interests representative.
[48] Chapter H-0.021* of the Statutes of Saskatchewan, 1999 (effective September 1, 2003, except for subsections 17(1), 18(2) and (4) and section 69) as amended by the Statutes of Saskatchewan, 2002, c.R-8.2; 2003, c.25; 2004, c.A-26.1; 2004, c.65; 2005, c.Y-1.1; 2006, c.C-1.1 and c.19; 2008, c.V-7.3; 2009, c.32; 2013, c.W-17.11; 2014, c.16, c.E-13.1 and c.17; 2015, c.A-26.11, c.M-23.001, c.11, c.12 and c.17; 2016, c.P-4.11; 2017, c.P-30.3; 2018, c.42; and 2020, c.13.
[49] Report of Saskatchewan's Health Records Protection Working Group to the Deputy Minister of Health.
[50] *Ibid.,* at pp. 3 and 4.

intended as an option of first resort.[51]

To deter the abandonment of records, the WG recommended a strict liability offence (below) for abandonment of records be included in HIPA. They described the need for this type of offence as necessary to "sharply focus the compliance requirements and clarify the policy position with respect to securing personal health information" and to "[highlight] the consequences of non-compliance and [bring] home the intended deterrent to trustees and their employees".

(i) Strict Liability Offence

The Working Group recommends that HIPA be amended to provide for a new strict liability offence specifically aimed at addressing the issue of abandoned Personal Health Information (PHI). Our legislative review reflects that this proposed provision would be unique to Saskatchewan. The Working Group is, nevertheless, of the view that it is important in this context to make a clear statement to trustees and information service providers that a failure to protect PHI will constitute a prima facie offence unless they can establish that they have taken all reasonable steps to prevent that contravention.[52]

They added the following about how the provision would operate.

This provision would be unique in that it moves beyond the specific intent required elsewhere in the Act necessary to constitute an offence. In other words, it is not enough for a trustee to assert that they did not intend for PHI to be abandoned; they must show that they took all reasonable steps to avoid having PHI abandoned.

If they are able to establish that they took all reasonable steps, then they will have a substantive defence to a charge under this new section. The Working Group feels that this is consistent with the public policy goals intended to address this issue. Negligence, incompetence or simple indifference should not be enough to defeat a charge of abandoning or manifestly failing to protect PHI in accordance with requirements of HIPA. Due diligence is required from every trustee or information management service provider that is entrusted with PHI in Saskatchewan. This new offence would both reflect and support that policy.[53]

To facilitate the transfer of patient records when a trustee ceases operations, the WG identified that there is a need for a good transfer of records system in place that will assist trustees to provide secure storage and management of their records. Specifically, they noted that:[54]

- the system must be able to respond quickly and take control of the records;[55]

[51] Report, at p.5.
[52] *Ibid.*, at p. 7.
[53] *Ibid.,* at p. 8
[54] *Ibid.*, at p. 16.
[55] *Ibid.*

- there must be a place for the records to be taken for safe handling, such as a single facility that would have in place standard practices and efficiencies for handling the records and which would give affected patients a consistent place to go to obtain records;[56]

- having a single facility will facilitate the timely transfer of records when a trustee fails to fulfill their transfer obligations and the Minister exercises their authority to appoint someone to take custody and control of the records;[57]

- the information management service providers (IMSP) that are designated archives (DA)[58] under the current model can refuse to accept records;[59]

- the costs associated with storing and managing the records as well as responding to access or corrections requests has created an unwillingness by IMSP DAs to accept records;[60] and

- trustees may not be willing to pay for these services and there is no public funding to pay for them.[61]

To improve the transfer of records system, they recommended that[62] :

> [a]*t least one of the designated archives should be required to accept records offered by trustees…*

and,

> [t]*he costs associated with transferring the records to the designated archive should remain the responsibility of the trustee who is leaving the field. A system should be developed to ensure that the funds required covering the costs of the designated archive services are paid by the trustee in some fashion. The Working Group is not unanimous on how this would be accomplished, but the discussion noted the following:*
>
> *a. For trustees that are regulated by a professional regulatory authority, the professional regulatory authority could levy annual fees from the members and set up a fund to cover the costs associated with record storage where records are abandoned by their members. To facilitate member use of reasonable cost storage solutions, professional regulatory authorities could co-operate and procure bulk arrangements with private storage companies to establish reduced fees from those that members might obtain individually for the service.*
>
> *b. Many other trustees are required to be licensed to carry on their health operations (personal*

[56] *Ibid.*
[57] *Ibid.* at p. 17.
[58] IMSPs that are designated archives (DAs) existed in HIPA at the time the Report was prepared. Then, HIPA authorized a trustee to transfer the custody and control of their records to an IMSP DA when ceasing operations.
[59] *Ibid.* at p. 18.
[60] *Ibid.*
[61] *Ibid.* at p. 19.
[62] I have included only those recommendations that are applicable.

care homes, health facilities, ambulance operators, etc.). The terms and conditions associated with licensing could require trustees to demonstrate that they have an arrangement or plan to deal with patient records on winding up operations and additional licensing fees could be assessed for the purposes of establishing a fund that the licensing body can access in the event records of an operator are abandoned.

HIPA was amended following the Report and the provisions to address the abandoned records were amended based on the recommendations of the Report.

HIPA

The model contained in HIPA for transfer of records by trustees when they cease practice is set out below.

Continuing duties of trustees

22(1) Where a trustee ceases to be a trustee with respect to any records containing personal health information, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee continue to apply to the former trustee until the former trustee transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

(2) Where a former trustee fails to carry out the duties continued pursuant to subsection (1), the minister may appoint a person or body to act in place of the former trustee until custody and control of the personal health information is transferred to another trustee or to an information management service provider that is a designated archive.

(2.1) If a trustee fails to keep secure personal health information in the custody or control of the trustee, the minister may appoint a person or body to act in place of the trustee until custody or control of the personal health information is re-established, transferred to another trustee or transferred to an information management service provider that is a designated archive.

(3) Where a trustee dies, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee become the duties of the personal representative of the trustee and continue to apply to the personal representative until the personal representative transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

"Designated archive" means an archive designated in the regulations for the purposes of section 22.

"Information management service provider" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any

of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf.

Information management service provider

18(1) A trustee may provide personal health information to an information management service provider:

(c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee;

(3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

The *Health Information Protection Regulations*[63]

Designated archives

4(1) For the purposes of section 22 of the Act, the following are designated archives:

(a) affiliates;

(b) the Ministry of Health;

(c) health professional bodies that regulate members of a health profession pursuant to an Act;

(d) the provincial health authority;

(e) Saskatchewan Archives Board;

(f) eHealth Saskatchewan;

(g) University of Regina Archives;

(h) University of Saskatchewan Archives.

(2) Nothing in this section requires a designated archive to accept personal health information

[63] Chapter H-0.021 Reg 1 (effective July 22, 2005) as amended by Saskatchewan Regulations 20/2007, 28/2010, 6/2014, 25/2015, 14/2016, 115/2017 and 61/2018.

from a trustee.

The following offence was added.

Offences

64 (1.1) No trustee or information management service provider, or former trustee or information management service provider, shall fail to keep secure the personal health information in its custody or control as required by this Act.

(1.2) No person shall be found to have contravened subsection (1.1) if that person can establish that he or she took all reasonable steps to prevent the contravention.

(2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:

(a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and

(b) in the case of a corporation, to a fine of not more than $500,000.

While the model in Saskatchewan's HIPA has some positive aspects to it, in my view, there are some gaps that may result in records not being transferred which creates risks for individuals of a privacy breach and from not being able to locate their records. For example, there is no requirement that a trustee transfers their records.

The proposed model

Under HIPMA, custodians should be required to transfer their records to another custodian or a custodian that is a designated archive (CDA) within a reasonable period of time after ceasing operations.

A single CDA that is located in Yukon should be identified to provide certainty as to where the records are located in Yukon and who has established standards of practice for managing records received.

If the custodian after ceasing operations fails to transfer their records as required, the Minister should be required to transfer custody and control of the records to the CDA.

The CDA will have all the responsibilities of a custodian under HIPMA but its purposes of collection, use and disclosure of PHI will be limited to its purpose as a CDA, which on taking custody and control of the PHI is to:

1. store and protect the PHI;
2. notify individuals that their PHI has been transferred to the CDA;
3. facilitate the transfer of PHI to a custodian or health care provider in another jurisdiction if the individual requests transfer;

4. inform individuals of their right to have their record transferred to a custodian or health care provider in another jurisdiction;

5. transfer custody and control of the records to another custodian or health care provider of the individual's choosing;

6. inform individuals about the retention period of the record and when destruction will occur if not transferred;

7. inform individuals about their ability to exercise their right of access and correction to the PHI and to process such requests; and

8. manage complaints about its service;

Given the size of the Yukon's population and the sensitivity around the Department of Health and Social Services having access to the PHI of individuals who chose to receive services in the community, an option may be to designate Yukon Archives as the CDA for the Yukon.

Funding for their service would need to be addressed. In terms of funding, an option may be to build additional fees into registration for health care providers who practice in the Yukon and into licensing fees for businesses who are custodians.

The authority of the IPC to consider any non-compliance would need to be expanded to include any non-compliance by a CDA.

As a measure to deter non-compliance, a strict liability offence together with a due diligence defence should be added to the offence provisions in HIPMA.

Recommendation 7

To ensure that Yukoners' PHI is adequately protected when custodians cease their operations, I recommend that the proposed model, or something similar, be incorporated into HIPMA.

Requirement to adopt a security standard – section 19

Modern privacy legislation, such as the European Union's *General Data Protection Regulation* (GDPR), California's *California Consumer Privacy Act* (CCPA) and the United States' *Health Insurance Portability and Accountability Act* (HIPAA), include requirements to adopt an information security standard to protect PI or PHI. HIPAA resolves this problem by creating a so-called security crosswalk which refers to several standards that may be used to implement its required controls.[64] GDPR incorporates aspects of

[64] https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html.

ISO27001[65] and many companies use ISO27001 compliance and accreditation as a means to substantiate their compliance with GDPR's security standard requirements.[66] CCPA's regulator and enforcer, the California Attorney General, recommends the CIS[67] standard to meet CCPA's reasonable security requirement.[68] In Prince Edward Island's (PEI) *Health Information Act* (HIA) that went into force in 2020, there is a provision requiring custodians to adopt a security standard.

> *39. Protection of personal health information*
>
> *(1) A custodian shall protect personal health information by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.*
>
> *Idem - information practices (2)* ***The information practices referred to in subsection (1) shall be based on nationally or provincially recognized information technology and security standards and processes that are appropriate for the level of sensitivity of the personal health information to be protected****.*
>
> [emphasis added]

The advantage of adopting a specific information security standard to protect PHI, such as for example ISO27001, is threefold. Firstly, it sets a normative bar for evaluating administrative, technical and management controls to ensure confidentiality, integrity, and availability of PHI in a more granular and dynamic fashion.[69] Secondly, it gives custodians a way to prove that they are exercising due diligence for the PHI in their care. Thirdly, it gives the IPC, who is responsible for monitoring compliance with HIPMA, a standard to evaluate compliance against when investigating a complaint about inadequate safeguards or when auditing compliance with the same.

The risks to privacy of PHI are significant if it is not adequately protected. Most breaches of privacy occur because of a lack of adequate measures to protect PHI. As mentioned previously, because of the lack of incentives, through order making or other measures such as fines, custodians and organizations subject to privacy laws have no incentive to apply appropriate security safeguards and these laws have proven weak to enforce the same. It is cost-beneficial to them NOT to have proper information security safeguards because under many privacy laws, including HIPMA, there are no real consequences for inadequate safeguards, leaving the public exposed to risk.

The risks to privacy increase exponentially when technology is used to process PHI. Given our current environment in which a significant portion of PHI is processed digitally and the anticipated use of AI to process data, together with the use of the internet to transmit data, means that it is time for HIPMA to require a custodian to adopt an information security standard that is acceptable in its industry and to

---

[65] International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html.
[66] https://www.itgovernance.co.uk/gdpr-and-iso-27001.
[67] Cybersecurity standards developed by the Centre for Internet Security: https://www.cisecurity.org/controls/.
[68] https://www.stoelprivacyblog.com/2020/01/articles/uncategorized/ccpa-is-here-is-your-security-reasonable/.
[69] ISO standards get updated quite regularly to reflect changes in the environment such as the development of new technologies or methods that may compromise information security.

require the custodian to specify what the standard is in its statement of information practices.

Recommendation 8

To ensure the PHI in the custody or control of a custodian is adequately protected and for the purposes of more effectively evaluating compliance with security safeguards, it is recommended that custodians be required to adopt a nationally or internationally recognized information technology and security standard that is appropriate for the level of sensitivity of the PHI to be protected.

Recommendation 9

It is further recommended that the custodian be required to specify the standard adopted in its statement of information practices.

Information managers – section 51, regulation 21

Section 51 of HIPMA requires that custodians enter into an agreement with an information manager "…that provides for the protection of the information that is the subject of the services". Under HIPMA, information managers are an agent of the custodian and obligated to comply with HIPMA and the custodian's obligations thereunder by virtue of that status.

Information managers provide their services more and more with the help of sometimes dozens of third-party services, products and consultations. Health legislation, such as HIPAA, contain provisions to address the risks created by the use of third parties by information managers. HIPAA contains an 'Omnibus rule' for information managers (referred to as business associates under HIPAA). In HIPAA, information managers must ensure the third parties they deal with comply with these same legal obligations, creating a cascading effect regarding protection for PHI from custodian to information managers and their subcontractors, as far down the chain as the PHI that the custodian is responsible for is involved. The provision states as follows.

> *Covered entities that engage business associates to work on their behalf must have contracts or other arrangements in place with their business associates to ensure that the business associates safeguard protected health information, and use and disclose the information only as permitted or required by the Privacy Rule*.[70]

[70] https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf, at p. 5557.

Recommendation 10

To prevent violations of HIPMA that may occur as a result of an information manager's use of a third party to provide its services to a custodian, I recommend information managers be required to have contracts or other formal arrangements in place with a third party engaged by the information manager in the provision of its services to a custodian that requires the third party to protect any PHI to which it has access, in a manner that will meet or exceed the information manager's obligation to protect the PHI as required by its information manager agreement with the custodian.

Auditing requirement to ensure awareness of HIPMA – section 19, regulation 14(c)

Section 19 together with subsection 14 (c) of the Regulation requires custodians to at least every two years audit their information security safeguards including their information practices and procedures. We have developed an audit tool to support custodians in meeting this obligation and included a reference to the tool in our recently issued HIPMA Toolkit for Small Custodians. We have seen in practice custodians struggle to meet their obligations under HIPMA. We developed these resources to assist them. While the audit requirement exists, we have no way of knowing if these audits are being carried out and if so, what gaps are revealed through the audit process. It would be beneficial as a measure to facilitate compliance if custodians are required to submit their completed audits to the IPC for review and comment. The goal here would be for the IPC's office to assist custodians in meeting their information security obligations and better protect the PHI of Yukoners.

Recommendation 11

To ensure audits are being conducted by custodians as required by subsection 14 (c) of the Regulation and to promote compliance with HIPMA's information security obligations, I recommend that a provision be added to the Regulation requiring custodians to submit the audit of their information security safeguards carried out in accordance with subsection 14 (c) of the Regulation to the IPC for review and comment.

Enhancing user activity tracking requirement – subsection 22(3) and section 76

Logging and auditing of electronic records has many benefits for custodians. Effective auditing deters employees from snooping and enables the early detection of malicious action by insiders or outside

cyber criminals. The sensitivity of health records, increasing ubiquity of electronic forms of PHI, and the benefits of proper auditing substantiate the need for beefing up the provisions that ensure proper auditing by meeting current standards.

Currently subsection 22 (3) requires a custodian to create and maintain records of user activity but there is no requirement to audit these records. As a measure to ensure there is no unauthorized access to PHI by a user, HIPMA should contain a provision that requires custodians to audit user activity both proactively and reactively. They should also be required to document when audits occur and on which information system the audit was conducted and by whom.

The requirement in subsection 22 (3)(c) is for the record of user activity to be "of access by a person". From an audit perspective, it is not sufficient to just record access. If multiple employees access a record, but only one makes an unauthorized change, it will be impossible to prove which of the employees who accessed the record made the change. To remedy this problem, this provision should include a requirement to record both access and changes.

Lastly, the user identification requirement under paragraph 22 (3)(a) should clarify that user identification should be unique to a specific person. Access by generic accounts creates opaque logs and makes accountability by auditing unnecessarily difficult as it is not known which employee used the account. Without such a specification, the security rule of non-repudiation[71] can be circumvented.

Including a requirement in HIPMA for audits of user activity will act as a deterrent to unauthorized access, including by snoopers.

Recommendation 12

To better protect PHI against unauthorized access and to deter the same, I recommend that:

(a) custodians be required to:

- **i. establish a program to audit user activity randomly, on at least an annual basis, on each of its electronic information systems and to audit user activity whenever unauthorized user activity may be suspected;**
- **ii. document the system audited, when it was audited, by whom and why (i.e., a proactive or reactive audit); and**
- **iii. create and maintain records of any changes made to PHI by a user; and**

(b) a prohibition on the use of generic user accounts to access PHI be included in HIPMA.

[71] "Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.": https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation.

Mandatory Privacy Impact Assessment – Regulation section 15

Subsection 15 (1) of the Regulation requires two custodians, the Department of Health and Social Services and Yukon Hospital Corporation, to conduct Privacy Impact Assessments (PIAs) in the following circumstances:

> *a. prior to implementing any measure that, in the opinion of the Minister, is a significant change to an existing information system used to process PHI; or*
> b. *prior to commencing the operation of a new information system intended to be used to process PHI.*[72]

Subsection 15 (2) requires these custodians to submit a PIA conducted in accordance with subsection (1) "to the [IPC] before the information system is changed or its operation is commenced".

The addition of mandatory PIAs in HIPMA when it was enacted in 2016 was very positive. PIAs are recognized in Canada and internationally as one of the most effective tools to facilitate compliance with privacy laws when organizations plan to process PI. Most modern privacy laws contain a requirement to conduct PIAs and submit them to the appropriate oversight body for review and comment. Including this requirement in privacy law promotes accountability for compliance by organizations and promotes public trust.

A PIA is a tool that if used properly will facilitate compliance with privacy laws. What it does is 'bake in' privacy by design and reduces the likelihood of breaches.

When creating a PIA, the custodian is able to map the flow of personal information from collection to destruction or archiving (as applicable) and allows the custodian to establish legal authority for the collection, use, disclosure and management of the PI associated with the system used. A PIA also allows the person creating it to ensure the PI is secured in accordance with legal requirements and enables the identification of risks of non-compliance and measures to mitigate the risks.

A PIA is considered an 'evergreen' document in that it is to be used to update any changes to the flow of PI associated with the system or to its security.

These are the purposes served by the mandatory PIA provision in the Regulation.

In practice, we have discovered some shortcomings in the PIA provisions that should be modified so the provision can achieve its purposes.

Timing of review and response to recommendations

Over the past five years, the custodians who are obligated to submit PIAs to the IPC submitted numerous PIAs to the office. According to subsection 15 (2), custodians need only to submit the PIA to the IPC prior to changing or commencing an information system. The IPC's general powers under HIPMA

[72] Subsection 15 (2) of the Regulation.

allow her to comment on the PIAs received and to make recommendations.

In the early days, we received some PIAs within a very short time period before the information system on which the PIA was conducted was ready to go live. This was highly problematic. In some cases, we found non-compliance with the use of a system because of its design and would raise the issue with the custodian. These issues were not resolved. Our attempts to resolve them over the years has been unsuccessful. The only remedy for resolution is to replace the system or modify it so that its use will be compliant. We understand that there are significant costs associated with acquiring and implementing an electronic information system. It is not surprising that at the go-live stage, a custodian is unwilling to remedy non-compliance issues when doing so is cost-prohibitive. However, non-compliance based on cost is not an excuse that is acceptable in HIPMA. Because PHI is highly sensitive and the means of controlling one's own PHI is through the legal framework established in HIPMA, any non-compliance with HIPMA is an offence. A custodian cannot simply accept non-compliance, regardless of the circumstances. It is an offence to do so. Custodians must ensure that compliance with HIPMA is a key consideration in any procurement of information systems used to process PHI.

Over the past few years, the situation has improved significantly. Custodians are now engaging us early in the process, often during the planning stages before acquisition occurs, to ensure compliance with HIPMA can be achieved. Our compliance review team meets with custodians regularly to assist them in designing systems and processes that will be compliant. We meet regularly with Department staff who are responsible for conducting PIAs, which has proved a positive engagement to facilitate compliance.

The use of PIAs in the Yukon is relatively new and they can be complex. For the past several years, our office has worked closely with custodians and public bodies on their completion. It is encouraging that the employees in these bodies tasked to conduct PIAs have, over the years, become much more skilled, which has resulted in our acceptance of many more PIAs.

Prior to just a few years ago, we rarely accepted a PIA that was submitted to us for review. This acceptance means that we are satisfied there are no major non-compliance issues and that any minor ones identified can be addressed through risk recognition and mitigation measures.

Unfortunately, there are still PIAs that we have not accepted because we identified non-compliance risks, some significant, that were never addressed. The list of these PIAs is contained in each of my annual reports and is updated each year. The list from my 2019 annual report lists 16 PIAs that were submitted to our office for review between 2016 and 2019 that have not yet been accepted.

In recognition of some of the challenges we were experiencing with the PIA process, particularly around the lack of responses to issues raised, we recommended the new ATIPP Act, which contains a mandatory PIA provision, include a process that required a response to the IPC following its review of a PIA. Our recommendation was accepted and the process is set out in section 11 of the ATIPPA, as summarized below.

Subsection 11 (1) requires a public body to conduct a PIA for certain proposed activities and if there is a significant change to the collection, use or disclosure of PI by an existing program or activity or an

information management service.

Subsection 11 (2) requires the public body to "[w]ithin a reasonable period before a public body carries out or provides a proposal or change that is the subject of a [PIA]" the head of the public body must in certain circumstances provide a copy of the [PIA] to the IPC.

Subsection 11 (3) authorizes the IPC to provide recommendations to the head who conducted the PIA.

Subsection 11 (4) requires the head to "at least 20 days before the day on which the public body carries out or provides the proposal or change to which the recommendation relates, decide whether to accept or reject the recommendation and notify the IPC of their decision."

Subsection 11 (5) deems the failure to notify the IPC of the head's decision as a rejection.

HIPMA should contain a similar process as a means to ensure the purposes of including mandatory PIAs in HIPMA will be achieved.

Meaning of terms

Another issue that we have identified is a lack of clarity regarding the meaning of "information system" and what constitutes a "significant change" to an information system.

There has been disagreement between my office and custodians as to what an information system is. It is our view that an information system is any system, no matter the form, that may be paper-based or electronic, that involves the collection, use, disclosure and management of PHI. There is also disagreement about what qualifies as a significant change to an existing information system that would trigger the requirement to do a PIA.

In a letter dated December 15, 2017 (Dec '17 Letter), we issued advice to the Department on the interpretation of paragraph 15 (2)(a). This provision requires a custodian to conduct a PIA before carrying out any measure that, in the Minister's opinion, is a significant change to an existing information system used to handle PHI.

The advice pertained to changes to the joint BC-Yukon information system, called Panorama. Panorama contains public health-related PHI about Yukon and BC residents. The system operates as an inter-jurisdictional eHealth public health information system that is shared by BC and the Yukon.

The data governance framework for Panorama is very complex and involves signatories to an information sharing agreement (ISA). The ISA is signed by health care bodies in BC including the BC Centre for Disease Control, the BC Ministry of Health, and all BC regional health authorities. The Department is also a signatory. The data governance framework includes a data governance committee (DGC). The DGC is comprised of representatives of all the signatories to the ISA. There are two representatives from the Department on the DGC. There is a privacy and security onboarding process established to add additional members to Panorama.

In 2017, we learned that Panorama was being extended to more than 100 First Nation health service organizations (FNSOs) and that a decision document was issued by the DGC that authorized a different approval process for the purpose of reducing the time it would take to onboard the many FNSOs.

We conducted an analysis to determine if the onboarding of the FNSOs and the modification in process to onboard them qualified as a measure that is a significant change to an existing information system and found that it did. We advised the Department that it should inform the Minister about the changes to Panorama so that she could render her opinion under paragraph 15 (2)(a). We received no response from the Department to the Dec '17 Letter and did not receive a PIA about the change.

I will note here that we have repeatedly asked for a PIA that demonstrates compliance with HIPMA as it relates to the data processed in Panorama since HIPMA went into effect in 2016. The PIA we received in 2014 was based on compliance with the ATIPPA, not HIPMA, as HIPMA was not yet in force and the regulations had not yet been drafted. As of the date of writing these comments, we have yet to receive a PIA to demonstrate that the Panorama information system complies with HIPMA. We were recently informed that one is in development.

Application of mandatory PIA requirement

The mandatory requirement to conduct PIAs only applies to the Department and Yukon Hospital Corporation (YHC). Both these custodians routinely submit PIAs to us. A problem we have encountered in this model is when a system operated by YHC or the Department interfaces with other custodians' systems, the PIA only addresses part of the equation.

On more than one occasion, I have been provided with a PIA by the Department or YHC that demonstrates their compliance but, on review, also demonstrates that the custodians' system with whom their system interfaces cannot comply. Some of these circumstances have led to us not accepting certain PIAs.

The way in which health care is delivered in the Yukon involves the interface of numerous electronic information systems that are operated by different custodians. As IPC, I am responsible to monitor compliance with HIPMA by all custodians. If I receive a PIA that involves the collection, use or disclosure by more than one custodian because of the information system interfaces, I require a PIA that addresses the authority for all custodians involved to collect, use and disclose PHI and for its security.

To address this gap, the mandatory requirement to submit PIAs should be expanded to require a PIA be submitted by any custodian whose information system interfaces with an information system operated by the Department or YHC.

Expanding the application to submit a mandatory PIA in this manner does not mean that every custodian involved has to submit their own PIA. If the Department operates an information system that interfaces with other custodians, it would be required to submit a joint PIA that includes the authority of all participating custodians to collect, use and disclose PHI as part of the system interface and each custodian would be required to sign off that they agree with the authorities identified. The same

requirement would apply to YHC.

Recommendation 13

To ensure the purposes of completing PIAs under HIPMA is achieved, I recommend that:

- **(a) a custodian who submits a PIA to the IPC be required to respond to any recommendations made by the IPC in a specified time frame and before the system or change thereto goes live;**
- **(b) a custodian who fails to respond within the specified time frame be deemed to have refused the IPC's recommendations;**
- **(c) the terms "information system" and "significant change" in paragraph 15 (2)(a) and (b) of the *Health Information General Regulation* be defined; and**
- **(d) HIPMA requires any custodian whose information system interfaces with a system operated by the Department or YHC participate in the creation of the PIA to ensure that the custodian is meeting its obligations under HIPMA for any collection, use, access, disclosure that may occur as a result of the system interface and that the PHI is secured in accordance with HIPMA's requirements.**

Recommendation 14

In light of the risks to PHI as a result of the anticipated use of AI, I recommend that:

- **(a) the requirement to conduct a PIA is expanded to include any processing of PHI through the use of AI by any custodian; and**
- **(b) these custodians be required to submit these PIAs to the IPC for review and comment.**

Records retention and mobile devices – section 14(1), Regulation 17(d)

Increased use of mobile devices by custodians and their employees may negatively impact access and privacy rights for a number of reasons. The instant messaging feature on mobile devices is being used to schedule or provide the provision of care. When a custodian or their agent uses a business-issued device, the information is often not stored on institutional servers and there are, generally, no practices that ensure that this information is transferred to these servers. There is also no effective management of these messages, whether on a business or personal device, and in most cases these messages are deleted a short time after creation, making the information inaccessible.

The risks to privacy through use of instant messaging stems from poor security associated with the devices that are used and the fact that the information goes through a server of a third party. 'Bring your own device' policies create further privacy risks given that the line between personal and business

use is blurred and the information may become intertwined. The ability to store large amounts of personal information on mobile devices, including memory cards and USB flash drives, has resulted in a number of privacy breaches.[73]

Recommendation 15

To avoid these risks to privacy and to facilitate the right of access to PHI, I recommend that subsection 19 (3) be amended to restrict the use of digital devices that could or may contain any PHI of a custodian to custodian-issued devices and require a custodian to implement measures that:

- **(a) ensure that the PHI stored on these devices is transferred within a specified time period to the custodian's servers for management and access;**
- **(b) ensure that the PHI, once transferred, is deleted from the device;**
- **(c) ensure PHI on the device that is considered transitory is deleted from the device as soon as reasonably possible after its use; and**
- **(d) ensure the confidentiality, security and integrity of PHI stored on these devices is protected.**

Clarification of the CMOH as a custodian

Since the start of the pandemic, there has been a lack of clarity around whether the Chief Medical Officer of Health (CMOH) is a custodian and if or when he may be acting as an agent for the Department. To date the Department and IPC hold differing views on the matter. It would be useful to clarify the issue in HIPMA to ensure there is clear accountability for PHI that is collected by the CMOH and to ensure Yukoners know when he is responsible for their PHI so they can effectively exercise their right of access. I note that in Ontario's PHIPA, medical officers of health are expressly identified as health information custodians under that Act.

If the CMOH is identified as a custodian under HIPMA, it will be necessary to clarify when agents who are otherwise agents of the Department are acting as agents of the CMOH. Along with this will be the need to separate the management of PHI collected by agents of the CMOH from that of the Department. These agents must be trained to understand their roles as agents for the CMOH and Department to ensure that breaches of privacy do not occur as a result of unauthorized collections, uses or disclosure of PHI that may occur between the CMOH and the Department. As a custodian, in addition to his other duties under HIPMA, the CMOH will need to facilitate access to PHI and correction requests

[73] One of many examples: In September 2013, Medicentre Inc. reported the loss of a laptop containing the billing information of approximately 631,000 Albertans. The PI on the laptop included patient name, health number, birth date, diagnostic disease codes, and health service billing codes. The laptop was password protected but not encrypted. It was not recovered. Investigation Report H2014-IR-01 Report concerning theft of unencrypted laptop containing health information http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3481.

for any PHI in his custody or control.

Recommendation 16

To ensure that there is clear accountability for the work involving the CMOH, I recommend that this role in HIPMA be clarified.

Increasing compliance with HIPMA and public awareness

During the five years that HIPMA has been in effect, it has proven challenging for custodians to fulfill their duties under the Act. The IPC has produced and distributed a HIPMA audit tool to assist custodians in implementing requirements under the Act. We have also published and distributed various tools such as our small custodian toolkit and audit checklist to help custodians become aware and successfully fulfill their obligations under HIPMA. We also provide presentations for custodians and issued numerous responses to requests for advice regarding matters of HIPMA. We also proactively reach out to custodians when we notice their practices may not comply with HIPMA.

Part of the non-compliance we have encountered has been due to the complexity of HIPMA and the challenges faced by custodians in operationalizing its provisions. We have also perceived that there remains a general lack of understanding by Yukoners about their rights under HIPMA. Given this, consideration should be given to expanding the IPC's authority in areas to promote compliance and increase public awareness.

Recommendation 17

In addition to the IPC's investigation powers, it is recommended that the IPC be given the following general powers that are in addition to her power in section 92:

- **(a) power to consult with any person in respect of any matter relating to the purposes of HIPMA;**
- **(b) power to deliver educational programs, as necessary, for the purpose of informing the public of their rights under HIPMA and custodians of their duties under HIPMA;**
- **(c) provide on request of a person, reasonable assistance to the person in exercising their rights under HIPMA;**
- **(d) power to receive comments from the public in respect of a matter in relation to the protection of PHI or access to PHI under HIPMA, or a matter generally concerning the administration of HIPMA;**
- **(e) take actions that the IPC considers necessary to identify and promote changes to custodians' practices and procedures for improving the protection of PHI and**

access to PHI under HIPMA; and

(f) inform the public in respect of perceived deficiencies in the administration of HIPMA, including within the office of the IPC.

Offences and penalties

As part of this review, the offences and penalties provisions of HIPMA should be evaluated to determine if they are adequate to deter non-compliance.

In the current Act, there is an 'intent' component to most of the offences listed in the Act. To find that an offence occurred for a violation of the majority of HIPMA's provisions, it would have to be established that the person "knowingly" contravened the Act. Meeting this threshold can prove challenging, which not only reduces the likelihood that a person will be found to have committed an offence but also diminishes the deterrent effect of these provisions.

Offences

121(1) A person is guilty of an offence if the person

(a) in knowing contravention of this Act or the regulations

(i) collects, uses, discloses or accesses personal health information,
(ii) gains access to personal health information,
(iii) destroys or disposes of a record of personal health information,
(iv) collects or uses another person's Yukon public health insurance plan number, or
(v) requests the production of another person's YHCIP card

(b) knowingly fails to comply with any requirement under Division 3 of Part 3;

(c) in connection with the collection, use or disclosure of personal health information or access to a record of personal health information, makes an assertion, knowing that it is untrue, to the effect that the person is entitled to consent on behalf of another individual;

(d) alters, falsifies, conceals, destroys or erases any record, or directs another person to do so, with the intent to evade a request for access to the record;

(e) knowingly obstructs, makes a false statement to or misleads any person in that person's performance of their duties, powers or functions under this Act;

(f) knowingly breaches an agreement entered into with a custodian, including the Minister, if the agreement is required under this Act;

(g) knowingly contravenes (i) subsection 30(1), or (ii) any provision of Division 2 or 3 of

Part 7 or any requirement established under either of those Divisions; or

(h) contravenes section 118.

(2) A person who, otherwise than in an offence described in subsection (1), knowingly contravenes this Act or a regulation is guilty of an offence.

As can be seen by the table below, there is a trend in health information laws to remove the 'intent' component for certain offences. The most common offences where this has occurred are as follows.

1. Collecting, using or disclosing PHI contrary to the law.
2. Failing to take reasonable steps to safeguard PHI as required by the law.

Where these offences appear in health information laws, they are usually accompanied by a due diligence defence provision that enables a custodian to avoid being found guilty if they can establish that they took all reasonable steps to prevent the contravention.

There are a number of other notable offences in health information laws where the 'intent' component has also been eliminated. They are as follows.

1. Failing to comply with the breach notification provisions.
2. Disposing of or tampering with a record in order to evade an access request.
3. Contravening the restrictions related to a PHIN.
4. Violating the no-reprisal provisions.
5. Obstructing any person in the performance of their duties.
6. Breaching the terms and conditions of an agreement entered into.

If the transfer of records provisions are modified to require a custodian to transfer records on ceasing operations, then consideration should be given to including the 'failure to transfer records as required' as an offence.

The penalties for violation of HIPMA should also be reviewed. Currently, if a person is found guilty of an offence under HIPMA as described in subsection 121 (1), an individual is subject to a fine of up to $25,000 and for non-individuals up to $100,000. For knowingly violating the Act otherwise than under subsection 121 (1), a person is subject to a fine up to $500.00.

As can be seen from the comments above, the trend in privacy laws is to increase the fines to act as a deterrent to non-compliance. Bill C-11 (federal) and (Bill C-64 (Quebec) contain significant fines for non-compliance.

Bill C-11 contains fines that are the higher of $10 million and 3% of an organization's gross global revenue; and provides for a maximum fine not exceeding the higher of $25 million and 5% of an organization's gross global revenue in the case of a conviction for contravening certain specific provisions of the *Consumer Privacy Protection Act* or in the case of obstructing the Commissioner's work.

Bill C-64 contains fines of up to $10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions of up to $25 million or 4% of worldwide turnover.

The significant increase in the amount of these fines stems from the fact that the prior amounts did not act as a deterrent to large organizations from violating privacy laws and the recognition that fines needed to be significantly higher to achieve their deterrent effect. Also, the GDPR, on which these laws are based, has a similar fine, up to €20 million ($24.1 million) or 4% of annual global turnover (whichever is higher).

As can be seen from the table below, there is a wide range of penalties for non-compliance with privacy laws in Canadian jurisdictions that include fines and prison time. The new ATIPPA includes up to six months in prison as a penalty for non-compliance. What the correct penalties should be will need to be determined based on the specific Yukon context, the risks to the privacy of PHI in the digital environment, and the amount that is necessary to deter non-compliance as a measure to mitigate these risks in this environment. Consideration will also need to be given as to whether the fines in HIPMA will need to correlate in any way to those in PIPEDA's successor legislation to be substantially similar, should that status be sought.

Offences and penalties in health information laws in other jurisdictions in Canada[74]

Alberta's *Health Information Act*	<u>Offences</u> Threshold is knowingly with the following exceptions: 1) Failing to take reasonable steps to safeguard PHI is an offence. 2) Failing to comply with the breach notifications provisions by custodian or affiliate is an offence. <u>Penalties</u> Up $200,000 for an individual Up to $1,000,000 for any other person
Saskatchewan's *Health Information Protection Act*	<u>Offences</u> Threshold is a mix of knowingly and willfully with the following exceptions: 1) Falsely representing that a person is entitled to the PHI of another person is an offence. 2) Failing to secure the PHI as required is an offence. There is a due diligence defence for this offence with a threshold "took all reasonable steps to prevent the contravention" for this failure.

[74] See Appendix A for a complete listing of the offences and penalties in these jurisdictions.

	Penalties Up to $50,000 and/or one year in prison for individuals (includes directors of corporations) Up to $500,000 for a corporation
Manitoba's *Personal Health Information Act*	Offences Threshold is a mix of knowingly and willfully with the following exceptions: 1) Falsely representing that a person is entitled to the PHI of another person is an offence. 2) Collecting, using or disclosing a PHIN contrary to the Act is an offence. 3) Collecting, using, selling or disclosing PHI contrary to the Act or failing to protect the PHI as required are offences. There is a due diligence defence for these offences with a threshold "took all reasonable steps to prevent the contravention" for this failure. Penalties Up to $50,000 for all Contraventions found to be for more than one day are considered separate offences for each day that the contravention continues.
Ontario's *Personal Health Information Protection Act*	Offences Threshold is primarily willfully with the following exceptions: 1) Requesting access to or correction of PHI under false pretenses is an offence. 2) Contravening the restrictions on PHIN or obligations of the health data institute are offences. 3) Violating the non-retaliation provisions against employees is an offence. Penalties Up to $200,000 and/or one year in prison for a natural person Up to $1,000,0000 otherwise
New Brunswick's *Personal Health Information Privacy and Access Act*	Offences Threshold is mix of willful and knowingly thresholds with the following exceptions: 1) Obstructing the IPC is an offence. 2) Collecting, using, selling, or disclosing PHI contrary to the Act or failing

	to protect it as required are offences. There is a due diligence defence with a threshold "took all reasonable steps to prevent the contravention" for this failure. 3) Disclosing PHI contrary to the Act for a benefit to the custodian is an offence. 4) Violating the non-retaliation provisions against employees is an offence. <u>Penalties</u> Between $240 and $10,200 for all and for repeat convictions up to $15,000
Nova Scotia's *Personal Health Information Act*	<u>Offences</u> Threshold is willfully except for the following: 1) Failing to protect PHI as required is an offence. 2) Violating of the restrictions regarding the PHIN is an offence. 3) Using PHI for marking or commercial purposes without express consent is an offence. 4) Disclosing PHI contrary to the Act for a benefit to the custodian is an offence. 5) Breaching the terms and conditions of an agreement with a custodian is an offence. <u>Penalties</u> Up to $10,000 and/or six months in prison for individuals Up to $50,000 for corporations
PEI's *Health Information Act*	<u>Offences</u> 1) Failing or refusing to make PHI accessible via the PEI EHR as required is an offence. 2) Unauthorized access to certain PHI in the PEI EHR is an offence. 3) An employee or information manager who discloses PHI without authorization is guilty of an offence. 4) Any person who: collects, uses or discloses PHI contrary to the Act; sells PHI without authority; or fails to protect PHI as required is guilty of an offence. There is a due diligence defence for these offences with a threshold "took all reasonable steps to prevent the contravention" for this failure. 5) Any person who: discloses PHI for monetary or other benefit to the custodian; or takes an adverse measure against an employee in regard to the work of the IPC is guilty of an offence.

	Penalties For contravention of the Act or failure to comply with the IPC's orders: Up to $15,000 and/or six months in prison for individuals Up to $50,000 for corporations Contraventions or non-compliance with the IPC's orders found to be for more than one day are considered separate offences for each day it continues.
Newfoundland and Labrador's *Personal Health Information Act*	Offences Threshold is willfully except for the following: 1) Collecting, using or disclosing PHI contrary to the Act or failing to protect it as required is an offence. There is a due diligence defence for these offences with a threshold "took all reasonable steps to prevent the contravention" for this failure. 2) Disclosing PHI for monetary or other benefit to the custodian is an offence. Penalties Up to $10,000 and/or six months in prison for all
Northwest Territories *Health Information Act*	Offences Threshold is a mix of willfully and knowingly except for the following: 1) Misrepresenting authority to access a person's PHI or for making a change to it is an offence. Penalties Up to $50,000 for a person Up to $500,000 for corporations

There is no health information legislation in BC or Nunavut.

Recommendation 18

To ensure that the offence and penalty provisions are adequate to deter non-compliance, taking into account the current environment and the risks to PHI that will result from the anticipated use of advanced technology to process PHI, I recommend that these provisions be evaluated and revised as is necessary to ensure they will achieve their purpose in these environments.

Summary of recommendations

Recommendation 1

To ensure Yukon custodians are able to innovate in the delivery of health care by drawing on scientific and technological advances in health care delivery, it is recommended that HIPMA be amended to facilitate this innovation, taking into account the following:

(a) the social and environmental developments evolving as a result of the pandemic that have had and will continue to have a significant impact on the ability of individuals to meaningfully control their PHI;
(b) the impact on the health system that will emerge as a result of aging populations;
(c) the digital transformation that will impact how health care is delivered;
(d) advances in personalized medicine;
(e) the risks to privacy in this environment including from the emergence of the illegal trade in PHI and from foreign actors; and
(f) the modernization of privacy laws in Canada and internationally to address the risks to privacy stemming from the digital environment wherein PHI is being processed.

Recommendation 2

To ensure Yukoners' privacy rights will be protected in an environment where their PHI is processed through the use of technology designed to enhance health care delivery, it is recommended that the IPC be given the following powers:

(a) order-making power to remedy *any* non-compliance with HIPMA, or in the alternative the power to defer a refusal by a custodian to accept a recommendation to an adjudicator who has order-making power or the power to take a custodian to court if they refuse a recommendation;
(b) the same powers of a board of inquiry under the *Public Inquiries Act*;
(c) power to investigate *any* suspected violation of HIPMA on the IPC's own motion;
(d) power to conduct compliance audits;
(e) expanded investigative powers that apply to investigations and audits that include:
    i. the same power as is vested in the court to summon a person to appear before the IPC;
    ii. the same power as is vested in a court to compel a person summoned to give oral or written testimony;
    iii. the same power as is vested in a court to compel a person to produce to the IPC information or a record that in the opinion of the IPC is relevant to the investigation;
    iv. the same power as is vested in the court to examine information or a record that is produced to the IPC;
    v. power to enter any premises occupied by a custodian on satisfying any security

requirements of the custodian relating to the premises;

vi. power to converse in private with any person in the custodian's premises;
vii. power to conduct interviews with any person that the IPC reasonably believes may know or hold information that is relevant to an investigation;
viii. power to receive and consider evidence of any other type that in the opinion of the IPC may be relevant to the investigation or audit, whether or not the evidence would be admissible in a proceeding before a court;
ix. in respect of a matter under investigation, the power to determine each question of fact and law arising in relation to the matter;
x. power to join two or more complaints related to the same or similar matters for the purpose of conducting a single investigation into the complaints; and
xi. power to administer oaths.

Recommendation 3

I recommend that the scope of application of HIPMA in section 7 be evaluated to ensure all those subject to the Act by virtue of their obligations thereunder or in regard to its prohibitions are captured within this provision.

Recommendation 4

To alleviate the pressures on private sector custodians to comply with multiple privacy laws, I recommend that the Yukon government seek to have HIPMA declared substantially similar to PIPEDA or its successor legislation.

Recommendation 5

To provide Yukoners with the right to access social service records under public sector privacy law as is the case in every other jurisdiction in Canada, I recommend that HIPMA be revised to remove the application of HIPMA to social services records that are collected by or that are in the custody and control of the Department of Health and Social Services.

Recommendation 6

To ensure individuals can exercise effective control of their PHI, it is recommended that:

(a) the authority of a public body custodian to collect PHI without consent be removed from HIPMA; or
(b) if this authority remains, it is recommended that custodians who exercise this authority be required to provide notice to the individual about the collection, which notice must at minimum include:
    i. the purpose of the collection;
    ii. the authority for collection;

iii. that the PHI is being collected without consent;
iv. the right to refuse the collection;
v. the name and contact information of the custodian's contact individual to exercise their right of refusal or to answer any questions about the collection and right of refusal; and
vi. information about how to make a complaint to the IPC if the individual believes that the collection is not authorized.

Recommendation 7

To ensure that Yukoners' PHI is adequately protected when custodians cease their operations, I recommend that the proposed model, or something similar, be incorporated into HIPMA.

Recommendation 8

To ensure the PHI in the custody or control of a custodian is adequately protected and for the purposes of more effectively evaluating compliance, it is recommended that custodians be required to adopt a nationally or internationally recognized information technology and security standard that is appropriate for the level of sensitivity of the PHI to be protected.

Recommendation 9

It is further recommended that the custodian be required to specify the standard adopted in its statement of information practices.

Recommendation 10

To prevent violations of HIPMA that may occur as a result of an information manager's use of a third party to provide its services to a custodian, I recommend information managers be required to have contracts or other formal arrangements in place with a third party engaged by the information manager in the provision of its services to a custodian that requires the third party to protect any PHI to which it has access, in a manner that will meet or exceed the information manager's obligation to protect the PHI as required by its information manager agreement with the custodian.

Recommendation 11

To ensure audits are being conducted by custodians as required by subsection 14 (c) of the Regulation and to promote compliance with HIPMA's information security obligations, I recommend that a provision be added to the Regulation requiring custodians to submit the audit of their information security safeguards carried out in accordance with subsection 14 (c) of the Regulation to the IPC for review and comment.

Recommendation 12

To better protect PHI against unauthorized access and to deter the same, I recommend that:

(a) custodians be required to:
    i. establish a program to audit user activity randomly, on at least an annual basis, on each of its electronic information systems and to audit user activity whenever unauthorized user activity may be suspected;
    ii. document the system audited, when it was audited, by whom and why (i.e., a proactive or reactive audit); and
    iii. create and maintain records of any changes made to PHI by a user; and
(b) a prohibition on the use of generic user accounts to access PHI be included in HIPMA.

Recommendation 13

To ensure the purposes of completing PIAs under HIPMA is achieved, I recommend that:

(a) a custodian who submits a PIA to the IPC be required to respond to any recommendations made by the IPC in a specified time frame and before the system or change thereto goes live;
(b) a custodian who fails to respond within the specified time frame be deemed to have refused the IPC's recommendations;
(c) the terms "information system" and "significant change" in paragraph 15 (2)(a) and (b) of the *Health Information General Regulation* be defined; and
(d) HIPMA requires any custodian whose information system interfaces with a system operated by the Department or YHC participate in the creation of the PIA to ensure that the custodian is meeting its obligations under HIPMA for any collection, use, access, disclosure that may occur as a result of the system interface and that the PHI is secured in accordance with HIPMA's requirements.

Recommendation 14

In light of the risks to PHI as a result of the anticipated use of AI, I recommend that:

(a) the requirement to conduct a PIA is expanded to include any processing of PHI through the use of AI by any custodian; and
(b) these custodians be required to submit these PIAs to the IPC for review and comment.

Recommendation 15

To avoid these risks to privacy and to facilitate the right of access to PHI, I recommend that subsection 19 (3) be amended to restrict the use of digital devices that could or may contain any PHI of a custodian to custodian-issued devices and require a custodian to implement measures that:

(a) ensure that the PHI stored on these devices is transferred within a specified time period to the custodian's servers for management and access;

(b) ensure that the PHI, once transferred, is deleted from the device;
(c) ensure PHI on the device that is considered transitory is deleted from the device as soon as reasonably possible after its use; and
(d) ensure the confidentiality, security and integrity of PHI stored on these devices is protected.

Recommendation 16

To ensure that there is clear accountability for the work involving the CMOH, I recommend that this role in HIPMA be clarified.

Recommendation 17

In addition to the IPC's investigation powers, it is recommended that the IPC be given the following general powers that are in addition to her power in section 92:

(a) power to consult with any person in respect of any matter relating to the purposes of HIPMA;
(b) power to deliver educational programs, as necessary, for the purpose of informing the public of their rights under HIPMA and custodians of their duties under HIPMA;
(c) provide on request of a person, reasonable assistance to the person in exercising their rights under HIPMA;
(d) power to receive comments from the public in respect of a matter in relation to the protection of PHI or access to PHI under HIPMA, or a matter generally concerning the administration of HIPMA;
(e) take actions that the IPC considers necessary to identify and promote changes to custodians' practices and procedure for improving the protection of PHI and access to PHI under HIPMA; and
(f) inform the public in respect of perceived deficiencies in the administration of HIPMA, including within the office of the IPC.

Recommendation 18

To ensure that the offence and penalty provisions are adequate to deter non-compliance, taking into account the current environment and the risks to PHI that will result from the anticipated use of advanced technology to process PHI, I recommend that these provisions be evaluated and revised as is necessary to ensure they will achieve their purpose in these environments.